华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的“华为账号”和注册账号的“email地址”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训->面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- **4、学习工具 eNSP**
  - *eNSP (Enterprise Network Simulation Platform),* 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。**您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。**（http://support.huawei.com/ecommunity/bbs/list_2247.html）



华为认证网络工程师系列教程-HCNA

华为网络安全工程师认证

Huawei Certified Network Associate-Security



华为技术有限公司

华为认证网络工程师系列教程-HCNA

华为网络安全工程师认证

第2.0版本

华为认证系统介绍

依托华为公司雄厚的技术实力和专业的培训体系，华为认证考虑到不同客户对 ICT 技术不同层次的需求，致力于为客户提供实战性、专业化的技术认证。 根据 ICT 技术的特点和客户不同层次的需求，华为认证为客户提供面向十三个方向的四级认证体系。

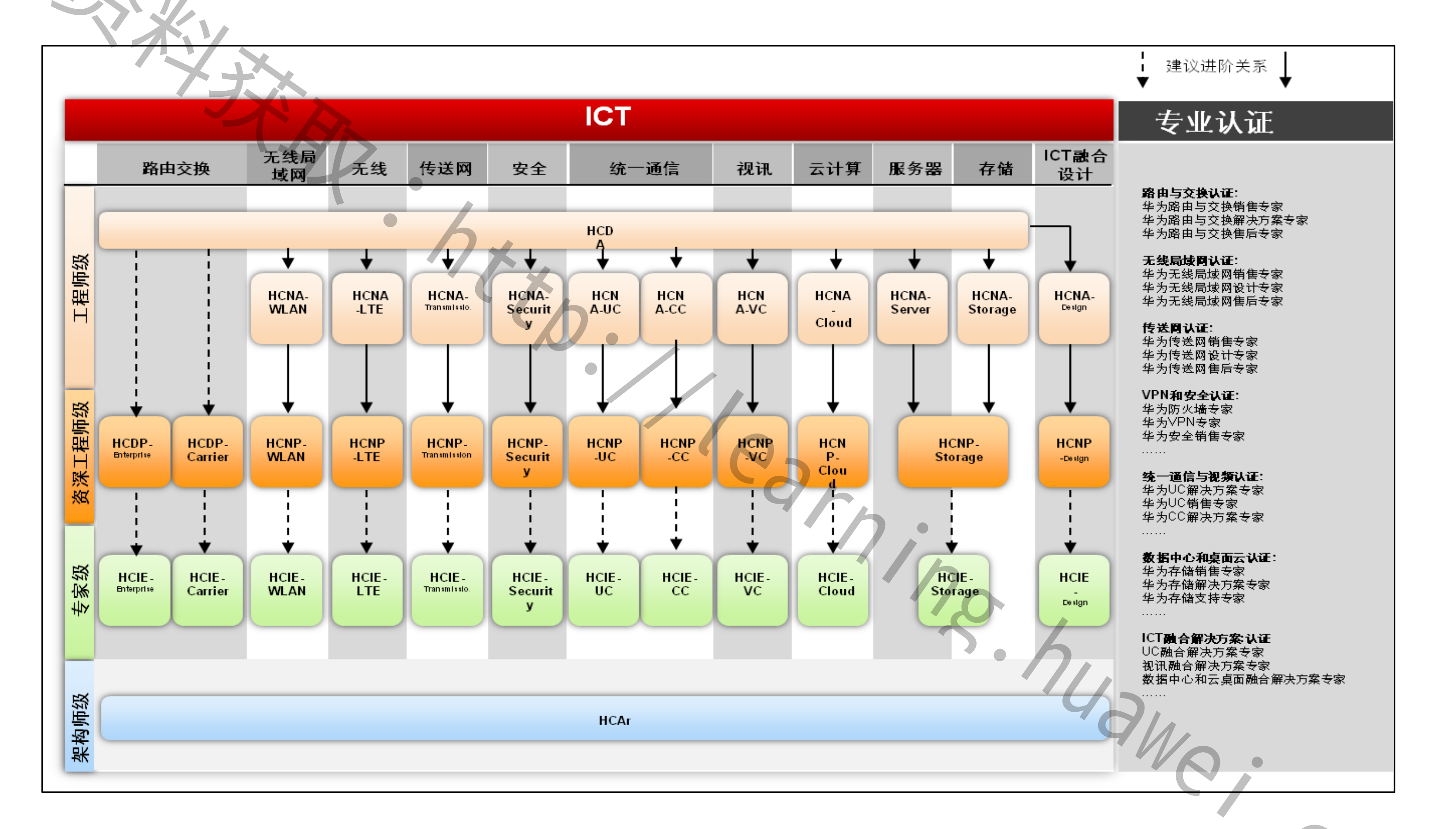
HCNA-Security（Huawei Certified Network Associate-Security，华为网络安全工程师认证）主要面向网络安全维护工程师，以及准备参加 HCNA-Security 认证考试的人员；希望掌握网络安全的基本原理和华为防火墙基本操作与部署能力的人员。HCNA 认证在内容上涵盖网络安全概述、防火墙基础技术、防火墙安全策略、网络地址转换技术、防火墙双机热备技术、防火墙用户管理、防火墙互联网技术、（L2TP、GRE、IPSec、SSL）VPN 技术、防火墙 UTM 技术、终端安全技术。

HCNP-Security (Huawei Certified Network Professional-Security，华为认证网络安全资深工程师)主要面向企业级网络安全维护工程师、专家工程师以及希望系统深入边界安全、终端安全、内容安全技术与部署的人员。

HCNP-Security 包括 CISN（Constructing Infrastructure of Security Network，构建安全网络架构）、CTSS（Constructing Terminal Security System，构建终端安全体系）、CSSN（Constructing Service Security Network，构建内容安全网络）三个部分。内容上涵盖防火墙高级技术（IP Car、IP-Link、Eth-Trunk、Link-Group、虚拟防火墙 VFW、双机热备高级技术、IPSec VPN、L2TP over IPSEC VPN 、DDOS 攻击防范技术及常见故障排除方法）、终端安全技术（TSM 技术、DSM 技术及常见故障处理方法）、UTM 技术（Anti Virus、IPS、Mail/Web/FTP Filtering、DPI 及常见的故障处理方法 ）。

HCIE-Security（Huawei Certified Internetwork Expert--Security，华为认证互联网络安全专家）旨在培养能够熟练掌握各种防火墙技术；精通华为安全产品的维护、诊断和故障排除；具备大型网络的安全规划、设计和优化的网络大师。

华为认证协助您打开行业之窗，开启改变之门，屹立在 ICT 世界的潮头浪尖！



建议进阶关系
ICT
专业认证
路由交换
无线局域网
无线
传送网
安全
统一通信
视讯
云计算
服务器
存储
ICT融合设计
工程师级
资深工程师级
专家级
架构师级
HCDA
HCNA-WLAN
HCNA-LTE
HCNA-Transmissio
HCNA-Security
HCNA-UC
HCNA-CC
HCNA-VC
HCNA-Cloud
HCNA-Server
HCNA-Storage
HCNA-Design
HCDP-Enterprise
HCDP-Carrier
HCNP-WLAN
HCNP-LTE
HCNP-Transmission
HCNP-Security
HCNP-UC
HCNP-CC
HCNP-VC
HCNP-Cloud
HCNP-Storage
HCNP-Design
HCIE-Enterprise
HCIE-Carrier
HCIE-WLAN
HCIE-LTE
HCIE-Transmissio
HCIE-Security
HCIE-UC
HCIE-CC
HCIE-VC
HCIE-Cloud
HCIE-Storage
HCIE-Design
HCAr
路由与交换认证:
华为路由与交换销售专家
华为路由与交换解决方案专家
华为路由与交换售后专家
无线局域网认证:
华为无线局域网销售专家
华为无线局域网设计专家
华为无线局域网售后专家
传送网认证:
华为传送网销售专家
华为传送网设计专家
华为传送网售后专家
VPN和安全认证:
华为防火墙专家
华为VPN专家
华为安全销售专家
……
统一通信与视频认证:
华为UC解决方案专家
华为UC销售专家
华为CC解决方案专家
……
数据中心和桌面云认证:
华为存储销售专家
华为存储解决方案专家
华为存储支持专家
……
ICT融合解决方案认证
UC融合解决方案专家
视讯融合解决方案专家
数据中心和云桌面融合解决方案专家
……

前言

简介

本书为 HCNA – Security 认证培训教程，适用于华为认证网络安全工程师以及准备参加 HCNA – Security 考试的学员或者希望系统掌握华为网络安全产品与技术的学员。

内容描述

本书共包含十二个 Module，系统地介绍了华为防火墙技术（防火墙基础技术、防火墙安全策略、网络地址转换技术、防火墙双机热备技术、防火墙用户管理、防火墙互联网技术、（L2TP、GRE、IPSec、SSL）VPN 技术、防火墙 UTM 技术、终端安全技术及其应用和常见的故障处理方法。

Module1 详细介绍了网络安全概述，主要包括 OST 模型、TCP/IP 协议原理、TCP/IP 协议存在的安全问题、常见的网络攻击方式。

Module 2 详细介绍了防火墙基础技术，主要有防火墙的定义、分类、主要功能、技术、转发数据流、基本配置。

Module 3 详细介绍了防火墙安全策略，主要包括防火墙包过滤技术、防火墙安全策略分类、应用场景及配置方法。

Module 4 详细介绍了网络地址转换技术，主要包括 NAT 的技术原理、不同的应用场景、NAT 配置。

Module 5 详细介绍了防火墙双机热备技术，主要包括：VRRP、VGMP、HRP 协议和典型场景的双机热备配置。

Module 6 详细介绍了防火墙用户管理，主要包括：用户认证技术、AAA 技术、用户认证管理的配置。

Module 7 详细介绍了防火墙互联网技术，主要包括 VLAN 的基本技术、SA 与 E1 广域接口技术、ADSL 的基本技术、WLAN 与 3G 无线技术。

Module 8 详细介绍了 VPN 技术基础；主要包括 VPN 概念、VPN 关键技术、VPN 分类及应用（L2TP 和 GRE）。

Module 9 详细介绍了 IPSEC VPN 技术，主要包括 IPSEC 技术的基本原理、应用场景及配置方法，安全协议 AH 与 ESP 技术介绍， IKE 协议的业务流程。

Module10 详细介绍了 SSL VPN 技术，主要包括 SSL VPN 的技术原理、配置方法及 SVN 产品的基本功能和特性。

Module 11 详细介绍了防火墙 UTM 技术，主要包括：防火墙 IPS 技术和防火墙 AV 网关防病毒技术及配置

Module 12 详细介绍了终端安全技术，主要包括终端安全定义、TSM 系统组成部份及部署、TSM 系统组织管理和准放控制方式、TSM 系统安全策配置。

本课程将引导学员完成所有 Module，学完本课程之后将具备 USG 系列防火墙和 TSM 产品基本规划和安装部署能力，以胜任网络安全工程师或系统管理员的工作岗位。

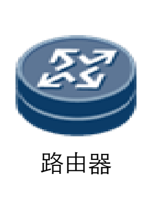
读者必备知识背景

本课程为华为网络安全认证基础课程，阅读本书的读者应首先具备以下基本条件之一：

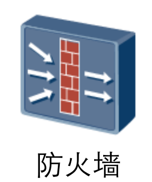
（1）熟悉数据通信网络的基础知识；

（2）具备一定的网络设备组网经验；

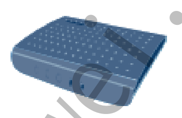
本书常用图标


路由器


交换机


防火墙


SVN



ADSL


PC

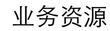

服务器



分支机构


网络终护


移动办公



业务资源


Email
服务器


DHCP
Server



Web服
务器












其它网络

目　录

HC110310001

HCNA-Security-CBSN 第一章 网络安全概述

第一章
网络安全概述

www.huawei.com

HUAWEI



目标

- 学完本课程后，您将能够:
  - 了解OSI模型
  - 理解TCP/IP协议原理
  - 了解TCP/IP协议存在的安全隐患
  - 理解针对TCP/IP各层常见攻击的技术原理





目录



OSI模型的提出

- OSI模型提出的目的
- OSI模型设计原则
- OSI模型的优点



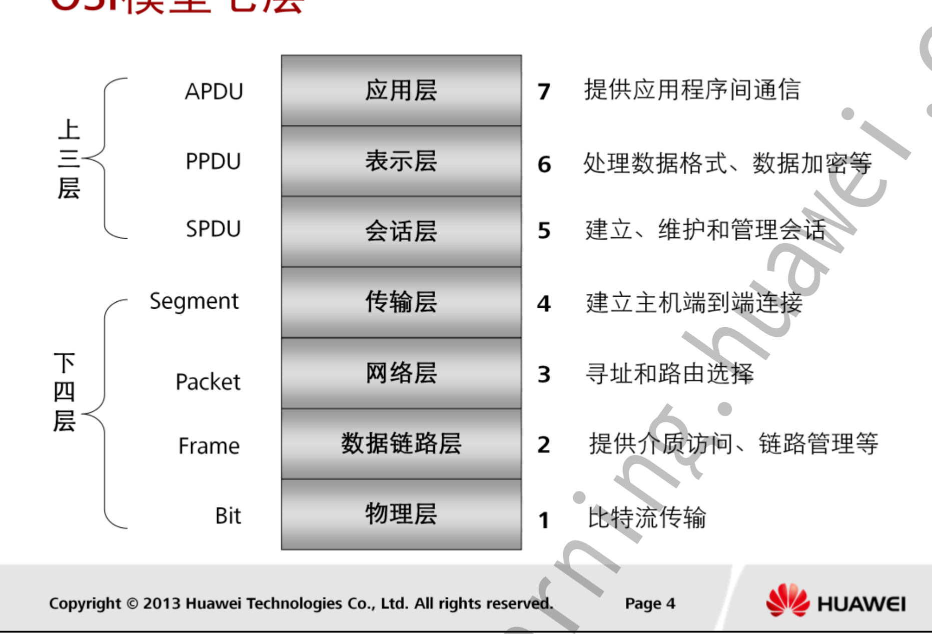
 Page 3



OSI:Open System Interconnect Reference Model，开放式系统互联参考模型。

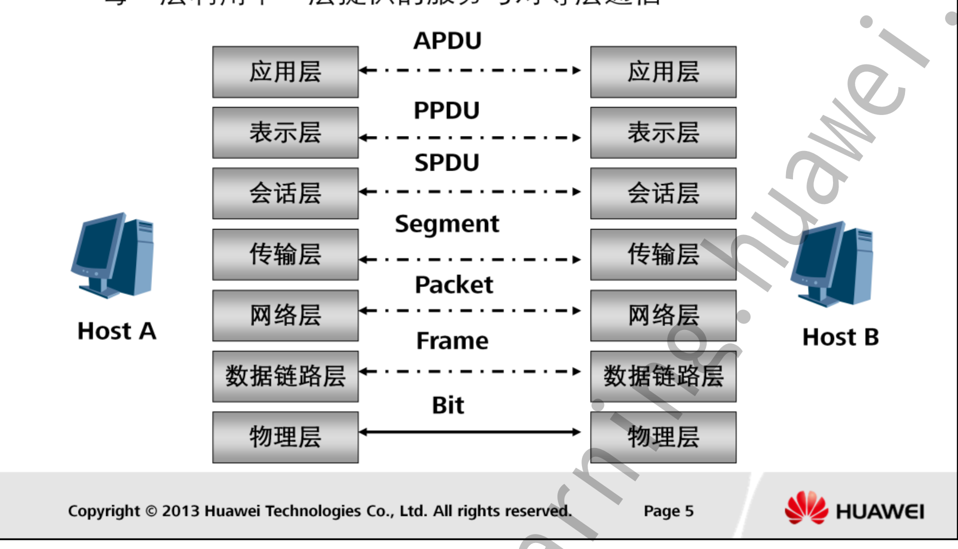
OSI模型的设计目的是成为一个开放网络互联模型，来克服使用众多网络模型所带来的互联困难和低效性。

- OSI参考模型很快成为计算机网络通信的基础模型。在设计时遵循了以下原则：
  - 各个层之间有清晰的边界，便于理解；
  - 每个层实现特定的功能，且相互不影响；
  - 每个层是服务者又是被服务者，即为上一层服务，又被下一层服务；
  - 层次的划分有利于国际标准协议的制定；
  - 层次的数目应该足够多，以避免各个层功能重复。
- OSI参考模型具有以下优点：
  - 简化了相关的网络操作；
  - 提供即插即用的兼容性和不同厂商之间的标准接口；
  - 使各个厂商能够设计出互操作的网络设备，加快数据通信网络发展；
  - 防止一个区域网络的变化影响另一个区域的网络，因此，每一个区域的网络都能单独快速升级；
  - 把复杂的网络问题分解为小的简单问题，易于学习和操作。



OSI七层模型中，给每一个对等层数据起一个统一的名字为：协议数据单元（PDU，Protocol Data Unit）。相应地，应用层数据称为应用层协议数据单元（APDU，Application Protocol Data Unit），表示层数据称为表示层协议数据单元（PPDU，Presentation Protocol Data Unit），会话层数据称为会话层协议数据单元（SPDU，Session Protocol Data Unit）。通常，我们把传输层数据称为段（Segment），网络层数据称为数据包（Packet），数据链路层称为帧（Frame），物理层数据称为比特流（Bit）。

封装（Encapsulation）是指网络节点（Node）将要传送的数据用特定的协议头打包，来传送数据，同样在某些层进行数据处理时，也会在数据尾部加上报文，这时候也称为封装。OSI七层模型的每一层都对数据进行封装，以保证数据能够正确无误的到达目的地，被终端主机接受、执行。



物理层涉及到在通信信道（channel）上传输的原始比特流，是OSI参考模型的基础，它实现传输数据所需要的机械、电气功能特性。它不关心每一bit流（0,1）所代表的含义（ 如：代表地址还是应用数据），只关注如何把bit流通过不同物理链路传输至对端。典型的象中继器、集线器（hub）就属于物理层设备。

链路层主要任务是提供对物理层的控制，检测并纠正可能出现的错误，使之对网络层显现一条无错线路，并且进行流量调控。

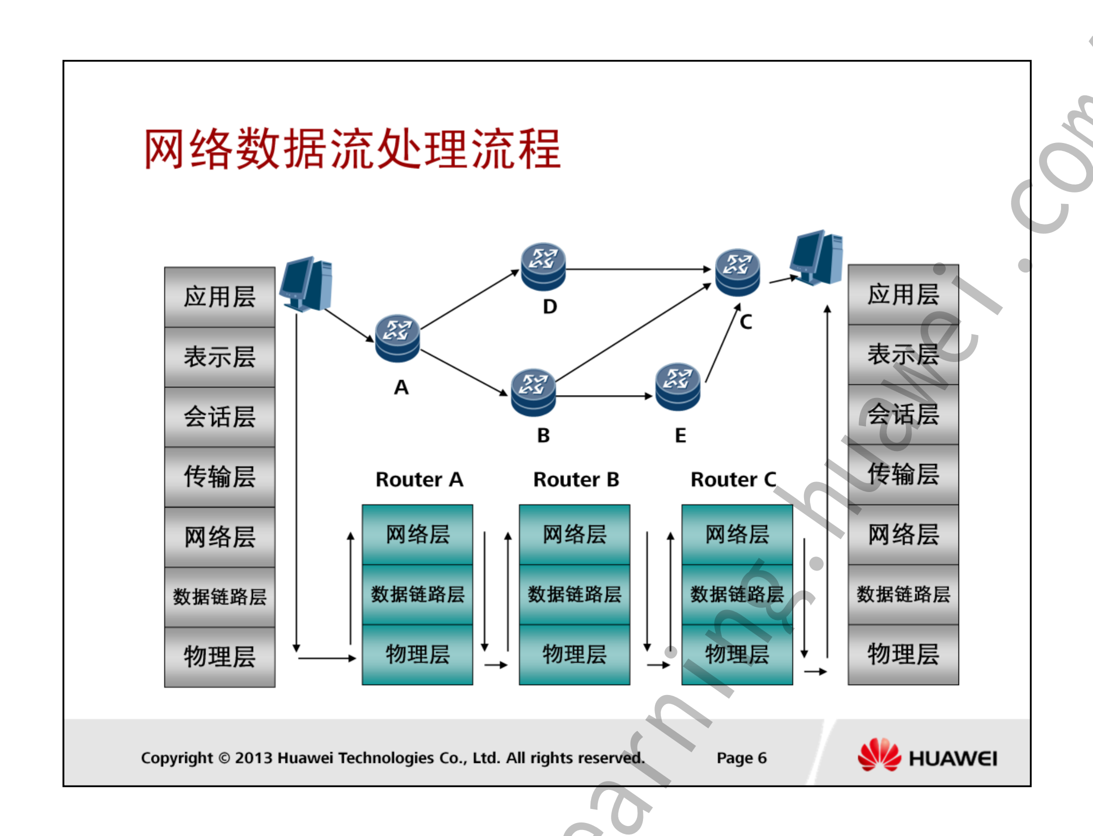
网络层检查网络拓扑，以决定传输报文的最佳路由，转发数据包。其关键问题是确定数据包从源端到目的端如何选择路由。网络层设备通过运行路由协议（Routing Protocol）来计算到目的地的最佳路由，找到数据包应该转发的下一个网络设备，然后利用网络层协议封装数据包，利用下层提供的服务把数据发送到下一个网络设备。

传输层位于OSI参考模型第四层，最终目标是向用户（一般指应用层的进程），提供有效、可靠的服务。

在会话层及以上的高层次中，数据传送的单位不再另外命名，统称为报文。会话层不参与具体的传输，它提供包括访问验证和会话管理在内的建立和维护应用之间通信的机制。如服务器验证用户登录便是由会话层完成的。

表示层主要解决用户信息的语法表示问题。它将欲交换的数据从适合于某一用户的抽象语法，转换为适合于OSI系统内部使用的传送语法。即提供格式化的表示和转换数据服务。数据的压缩和解压缩，加密和解密等工作都由表示层负责。

应用层为操作系统或网络应用程序提供访问网络服务的接口。



网络数据流处理过程：

1. 当某一网络的主机应用程序需要发送报文到位于另一个网络的主机时，与该主机在同一网络上的路由器的一个接口会接收到数据帧。
2. 路由器的链路层检查该帧，确定被携带的网络层数据类型，去掉链路层帧头，并将网络层数据送往相应的网络层进行处理。
3. 网络层检查报文头以决定目的地址所在网段，然后通过查找路由表以获取相应下一跳出接口。
4. 下一跳出接口的链路层为该报文加上链路层帧头，封装成数据帧并发送到下一跳。每一个报文的转发都要进行这一过程。
5. 在到达目的主机所在网络时，报文被封装成目的网络的链路层数据帧，发送给相应的目的主机。
6. 目的主机接收到该报文后，经过链路层、网络层的处理，去掉链路层帧头、网络层报文头后，送给相应的协议模块处理。

TCP/IP和OSI的对应关系

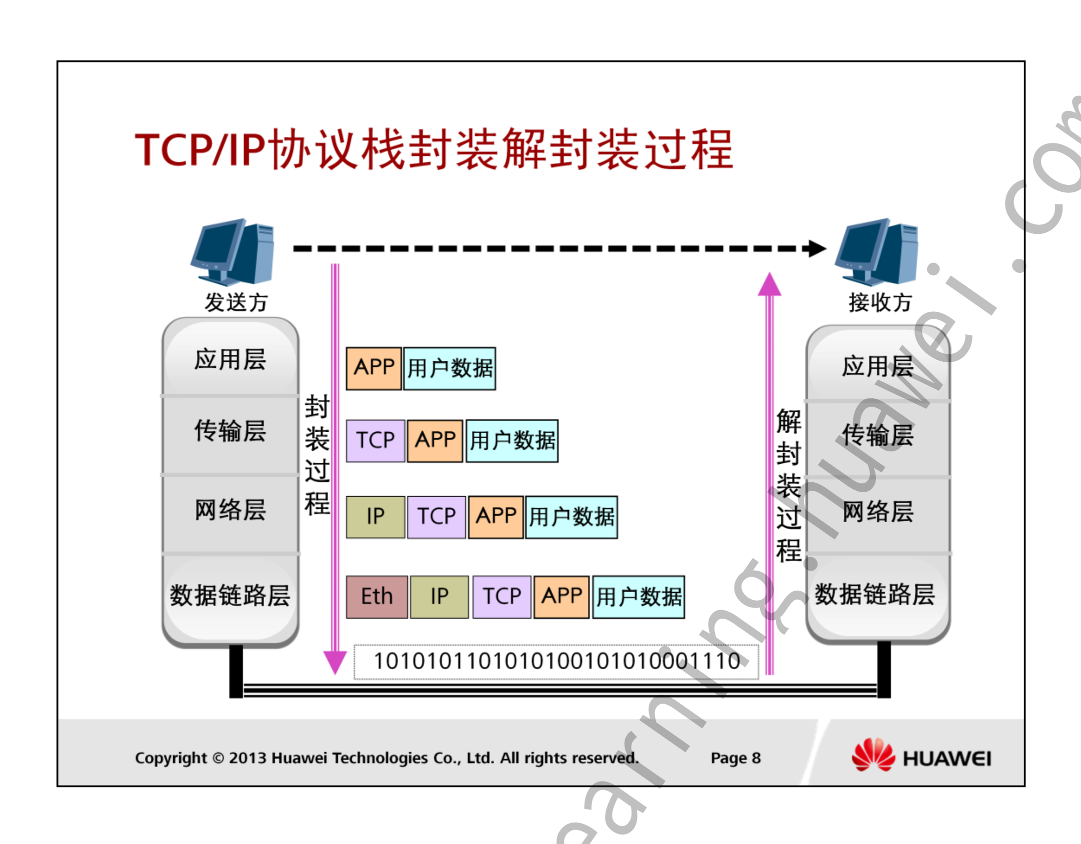
- TCP/IP协议栈具有简单的分层设计，与OSI参考模型有清晰的对应关系

OSI	TCP/IP
应用层	应用层
表示层	应用层
会话层	应用层
传输层	传输层
网络层	网络层
数据链路层	数据链路层
物理层	

 Page 7 HUAWEI

TCP/IP（Transfer Control Protocol/Internet Protocol，传输控制协议/网际协议）模型的开放性和易用性，以致在实践中得到了广泛应用，从而使TCP/IP协议栈事实上的标准协议。

TCP/IP模型与OSI参考模型的不同点在于TCP/IP把表示层和会话层都归入应用层，所以TCP/IP模型从下至上分为四层：数据链路层，网络层，传输层和应用层。在有些文献中也划分成五层，即把物理层也单独列出。



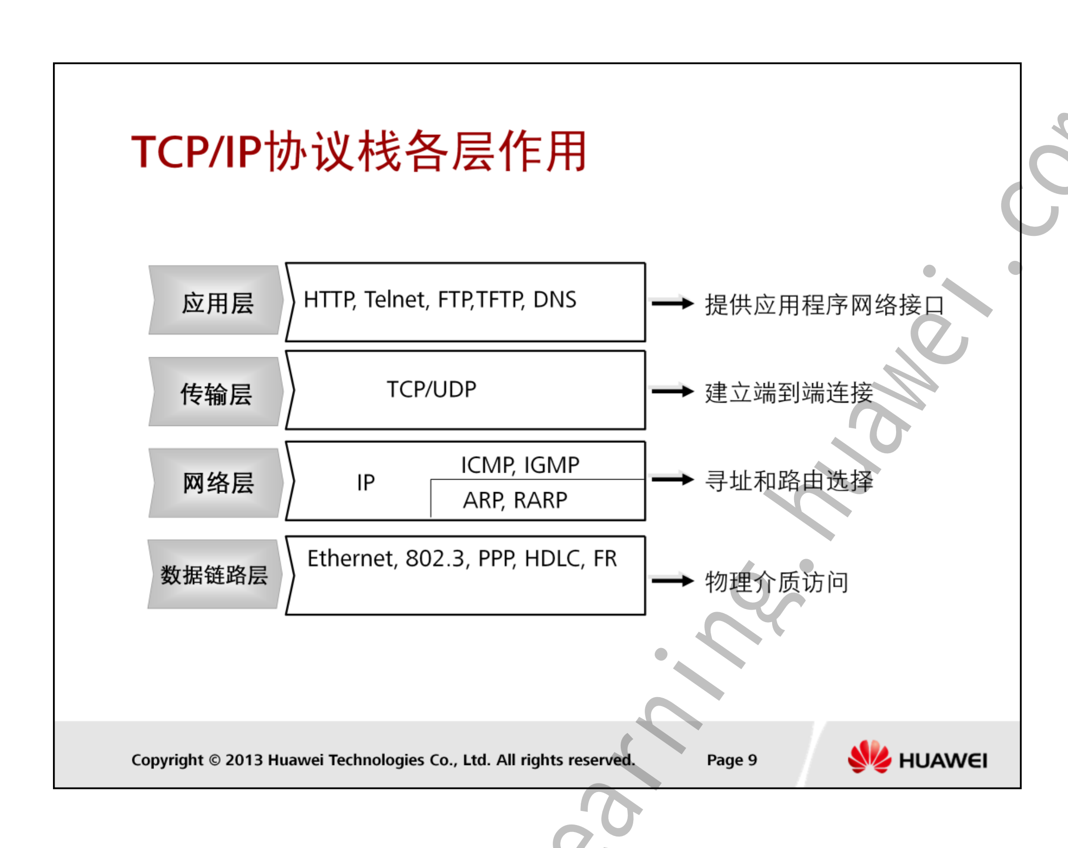
发送方将用户数据提交给应用程序把数据送达目的地，整个数据封装流程如下：

1. 用户数据首先传送至应用层，添加应用层信息；
2. 完成应用层处理后，数据将往下层传输层继续传送，添加传输层信息（如TCP或UDP，应用层协议已规定是TCP还是UDP）；
3. 完成传输层处理后，数据将往下层网络层继续传送，添加网络层信息（如IP）；
4. 完成网络层处理后，数据将往下层数据链接层继续传送，添加数据链层信息（如Ethernet、802.3、PPP、HDLC等），而后以比特流方式传输至对端（中间根据不同类型设备处理方式不同，交换机一般只进行数据链路层信息处理，而路由器进行更高层网络层处理，只有到达最终目的地才能恢复原用户数据）；

用户数据到达目的地后，将完成解封装流程：

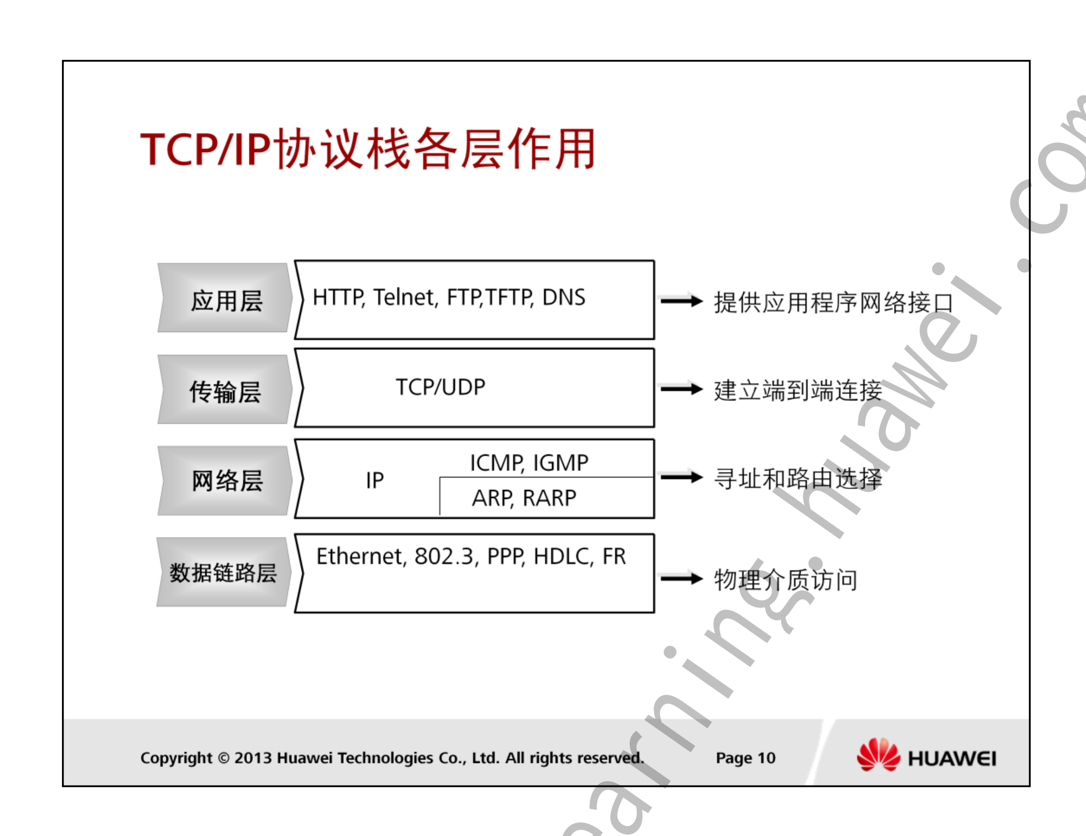
1. 数据包先传送至数据链路层，经过解析后数据链路层信息被剥离，并根据解析信息知道网络层信息，比如为IP；
2. 网络层接收数据包后，经过解析后网络层信息被剥离，并根据解析信息知道上层处理协议，比如TCP；
3. 传输层(TCP)接收数据包后，经过解析后传输层信息被剥离，并根据解析信息知道上层处理协议，比如HTTP；
4. 应用层接收到数据包后，经过解析后应用层信息被剥离，最终展示的用户数据与发送方主机发送的数据完全相同。

应用层和传输层提供端到端服务，网络层和数据链路层提供段到段服务。

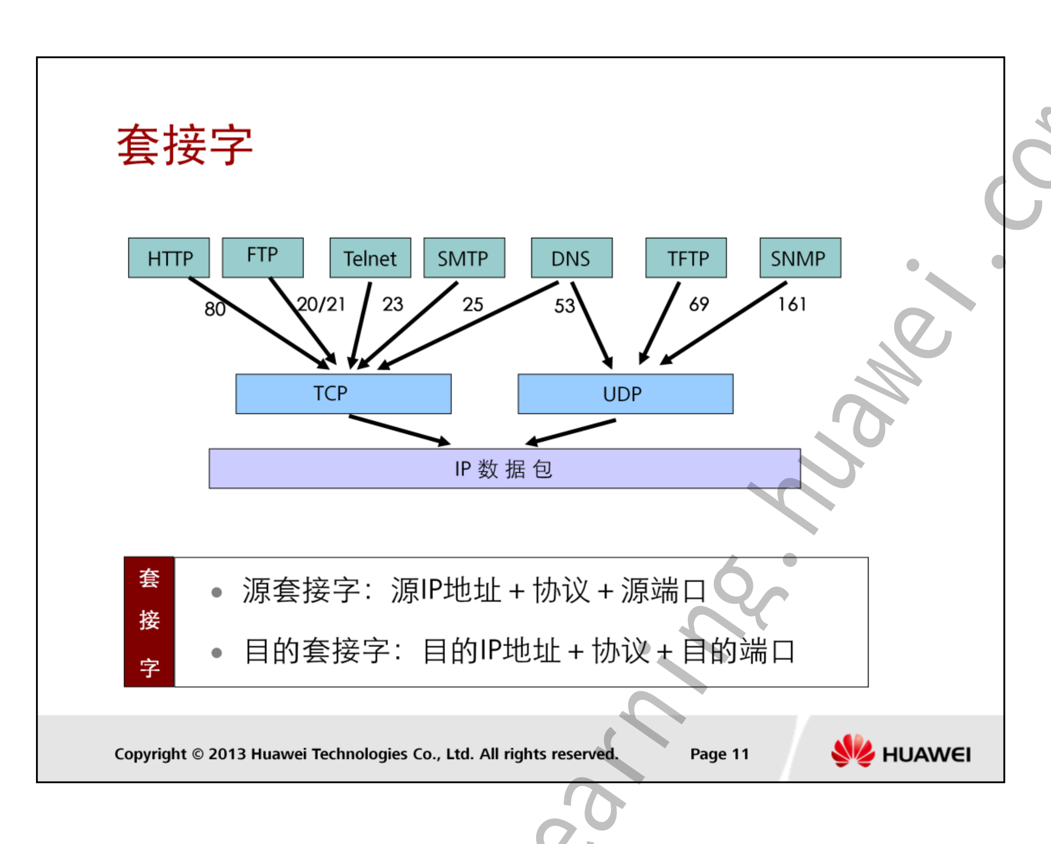


TCP/IP协议每一层都有对应的相关协议，且均为达成某一网络应用而产生，对于某些协议在分层上还不能严格对其定义。比如ICMP、IGMP、ARP、RARP协议我们把他们放在与网络层IP协议同一层。但在某些场合我们可能会把ICMP、IGMP放在IP协议的上层，而把ARP、RARP放在IP协议的下层。

- 应用层
  - HTTP（超文本传输协议）：用来访问在WWW服务器上的各种页面。
  - FTP（文件传输协议）：为文件传输提供了途径，它允许数据从一台主机传送到另一台主机上。
  - DNS（域名服务系统）：用于实现从主机域名到IP地址之间的转换。
- 传输层
  - TCP （传输控制协议） ：为应用程序提供可靠的面向连接的通信服务，适用于要求得到响应的应用程序。目前，许多流行的应用程序都使用TCP。
  - UDP（用户数据报协议）：提供了无连接通信，且不对传送数据包进行可靠的保证。适合于一次传输小量数据，可靠性则由应用层来负责。



- 网络层
  - IP（互联网协议）：IP协议和路由协议协同工作，寻找能够将数据包传送到目的端的最优路径。IP协议不关心数据报文的内容，提供无连接的、不可靠的服务。
  - ARP（地址解析协议）：把已知的IP地址解析为MAC地址。
  - RARP（反向地址解析协议）：用于数据链路层地址已知时，解析IP地址。
  - ICMP（网际控制消息协议）：定义了网络层控制和传递消息的功能。
  - IGMP（网际组管理协议）：用于组播组成员管理。
- 数据链路层
  - 数据链路层分为两个子层：逻辑链路控制子层（LLC, Logic Link Control Sublayer），介质访问控制子层（MAC, Media Access Control Sublayer）。



一个套接字由相关五元组构成：源IP地址、目的IP地址、协议、源端口、目的端口。其中协议信息，如TCP为6，UDP为17。

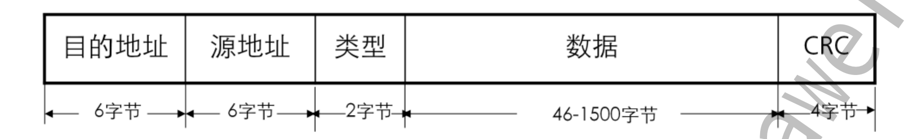
目的端口：一般知名的应用服务均会有标准的端口，比如HTTP、FTP、Telnet等，其中有些应用因非流行等原因，其端口一般由开发厂商自行定义，但要保证在同一台服务器注册的服务端口是唯一的。

源端口：一般都采用1024及以上端口进行递增分配，但某些操作系统可能会使用更高的端口号做为其初始端口进行递增分配。因源端口不可预知性，所以在ACL策略中比较少涉及。

任何应用服务器要想对外提供业务服务，均需在服务启动期间在TCP/UDP上进行端口注册，以便响应业务服务请求。通过五元组，应用服务器可响应任何并发服务请求，且能保证每一链接在本系统内是唯一的。

数据链路层协议

- 以太网协议封装



- 类型信息
  - 类型，0x0800：代表IP
  - 类型，0x0806：代表ARP
  - 类型，0x8035：代表RARP

 Page 12



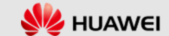
数据链路层协议在TCP/IP协议栈中，可以说是最低层协议。可分为局域网和广域网，我们在此只列出局域网协议的一种，广域网协议可参考其它互联网文献。

局域网协议，包括以太网、令牌网等。主要有两种帧格式，即以太网帧格式和802.3帧格式，目前以以太网帧格式应用为主。802.3帧格式相对比以太网帧格式复杂些，除了多提供长度字段外，还增加了其它类字段，不过此两类帧格式对最小长度和最长长度均要求一致。

- 数据链路层协议主要包括以下功能：
  - 数据链路参数协调，比如双工、速率等；
  - 针对发送数据包负责封装数据帧头信息（可能还会有帧尾），针对接收数据包负责识别数据帧头信息，对于发给自身数据包进行解封装处理；
  - 对于大部分数据链路层协议，均具备侦错能力，但不支持纠错能力，纠错功能一般是由后面将讲述的传输层协议来提供，比如TCP协议。

网络层协议

0	4	8	16	19 — 31
版本	报文长度	服务类型	总 长 度	
标 识 符			标志	片 偏 移
生存时间TTL		协议	报 头 校 验 和	
源 IP 地 址				
目 的 IP 地 址				
IP 选 项				填充项

 Page 13 

- Version(版本):

  占4bit，标识IP 封包的版本，目前使用的是 IPv4;
- 报文长度（Header Length）：

  占4bit，描述IP包头的长度，单位为字节(bytes)
- 服务类型（Type of Service）：

  占8bit，前3个bit定义包的优先级，后5个bit分别表示为D 时延、 T 吞吐量、 R 可靠性、M 传输成本和0 保留位;
- IP包总长（Total Length）：

  占16bit，以字节为单位计算的IP包的长度 (包括头部和数据)，IP包最大长度65535字节
- 标识符（Identifier）：

  占16bit，该字段和Flags和Fragment Offset字段联合使用，对较大的上层数据包进行分段（fragment）操作;
- 标记（Flags）：

  占3bit，第1位不使用。第2位是DF（Don't Fragment）位，1表明不能对数据包分段，0表示可分段。第3位是MF（More Fragments）位，MF位为1表示该数据包为最后1个分段数据包。
- 片偏移（Fragment Offset）：

  占3bit，表示该IP包在该组分片包中位置;

网络层协议

0 版本	4 报文长度	8 服务类型	16	19 总长度	31
标识符			标志	片偏移	
生存时间TTL		协议	报头校验和		
源IP地址					
目的IP地址					
IP选项				填充项	

 Page 14 HUAWEI

- 生存时间（TTL）：

  占8bit，数据包每经过1个路由器会将IP包的TTL值减少1；

- 协议（Protocol）：

  占8bit，标识了上层所使用的协议。和端口号类似，IP协议用协议号区分上层协议。TCP协议的协议号为6，UDP协议的协议号为17。

- 报头校验和（Head checksum）：

  计算IP头部的校验和，检查报文头部的完整性；

- 源IP地址和目的IP地址：

  标识数据包的源端设备和目的端设备；

- 可选项（Options）：

  这是一个可变长的字段；

- 填充（Padding）：

  因为IP包头长度（Header Length）部分的单位为32bit，所以IP包头的长度必须为32bit的整数倍。因此，在可选项后面，IP协议会填充若干个0，以达到32bit的整数倍 。

传输层协议

0　　　　8	16　　　　24　　　　31
源端口	目的端口
UDP长度	UDP校验和（可选）
数据	

UDP报文格式

源端口									目的端口
序列号									
确认号									
首部长度	保留(6位)	URG	ACK	PSH	RST	SYN	FIN		窗口大小
TCP校验和									紧急指针
选项									
数据									

TCP报文格式

Page 15



UDP报文与TCP报文的格式有所不同，TCP明显比UDP长度更长，因此也相应有更多功能，比如可靠性等。TCP报文格式如下：

- Sequence Number：即发送序号。发送主机端会在TCP报文封装时，确定一个初始号码，后续报文序号会依次的递增，接收端可以根据此序号来检测报文是否接收完整。
- Acknowledgement Number ：即回应序号。接收端接收到TCP报文，通过检验确认之后会根据发送序号产生一个回应序号，发送端根据此序号确定报文被成功接收到。
- 源端口号（Source port）和目的端口号（Destination port）：用于标识和区分源端设备和目的端设备的应用进程。
- Data Offset ：报头固定长度。如果options没设定的话，其长度是20byte。
- Reserved ：这是保留区间暂时还没被使用。
- Contral Flag：包括六个标记位。
  - URG为1，表示紧急报文；
  - ACK为1，表示需要回应的报文；
  - PSH为1，此报文所携带的数据会直接上传给上层应用程序而无需经过TCP处理；
  - RST为1，要求重传；
  - SYN为1，表示要求双方进行同步沟通；
  - FIN为1，表示传送结束。

传输层协议

0 8	16 24 31
源端口	目的端口
UDP长度	UDP校验和（可选）
数据	

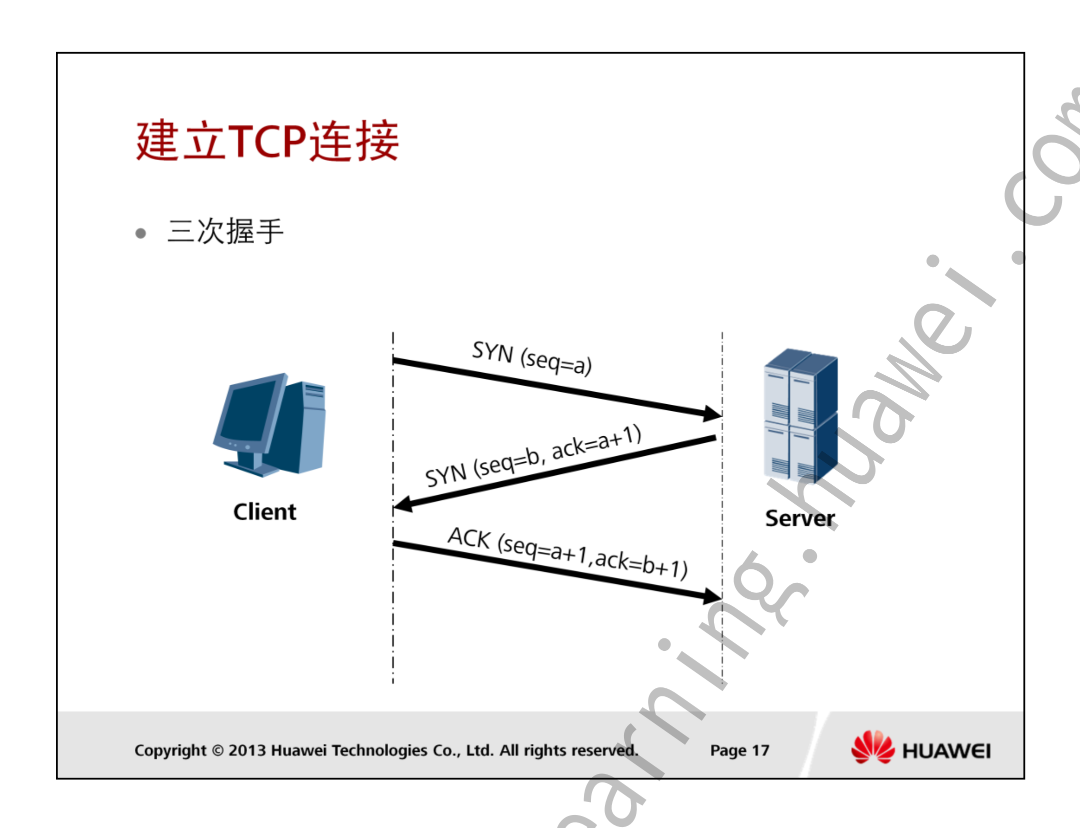
UDP报文格式

<table>
<tr><td colspan="8">源端口</td><td>目的端口</td></tr>
<tr><td colspan="9">序列号</td></tr>
<tr><td colspan="9">确认号</td></tr>
<tr><td>首部长度</td><td>保留(6位)</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>窗口大小</td></tr>
<tr><td colspan="8">TCP校验和</td><td>紧急指针</td></tr>
<tr><td colspan="9">选项</td></tr>
<tr><td colspan="9">数据</td></tr>
</table>

TCP报文格式

 Page 16 

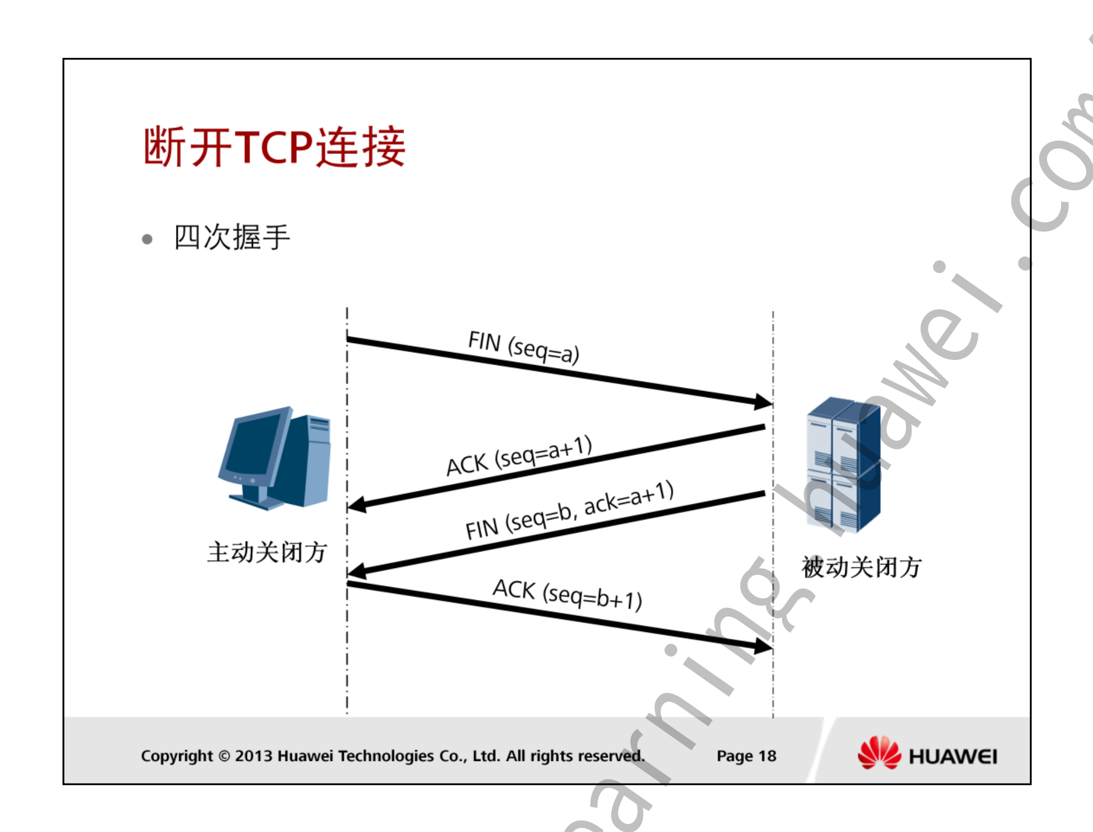
- 窗口大小：称为“滑动视窗(Sliding Window)”。当TCP连接建立起来后，两端都会将窗口大小设定为初始值，然后发送端就会按初始值大小（比如3）向对端发3个TCP报文，然后窗口会往后移动3个报文位，填补发送报文出去之后的空缺。如果接收端能一次处理接收下来的这3个报文的话，就会告诉发送端其窗口值为3，但如果接收端只能处理2个报文，就会告诉发送端其窗口值为2。这时，发送端需要调整其窗口大小为2，视窗则只会往后移动2个报文位，下一次只发送2个TCP报文。
- Chechsum ：当发送报文时，发送端会对报文进行计算得出一个检验值并和报文一起发送，接收端收到报文后，会再对报文进行计算，如果得出的值和检验值不一致，则会要求对方重发该个报文。
- Urgent Pointer ：如果URG被设定为1，这里就会指示出紧急报文所在位置，不过这种情形非常少见。
- Option ：这个选项比较少用。当需要使用同步动作的程序（如Telnet）要处理好终端的交互模式就会使用到option来指定报文的大小，因为telnet使用的报文很少但又需要即时回应。 Option的长度为0,或32bit的整倍数,如果不足则填充到满。



TCP的连接建立是一个三次握手过程，目的是为了通信双方确认开始序号，以便后续通信的有序进行。主要步骤如下：

1. 连接开始时，连接建立方(Client)发送SYN包，并包含了自己的初始序号a；
2. 连接接受方(Server)收到SYN包以后会回复一个SYN包，其中包含了对上一个a包的回应信息ACK，回应的序号为下一个希望收到包的序号，即a + 1，然后还包含了自己的初始序号b；
3. 连接建立方(Client)收到回应的SYN包以后，回复一个ACK包做响应，其中包含了下一个希望收到包的序号即b + 1。

经过此三次信息交换以后，TCP连接建立成功，就可以进行后续通信了。



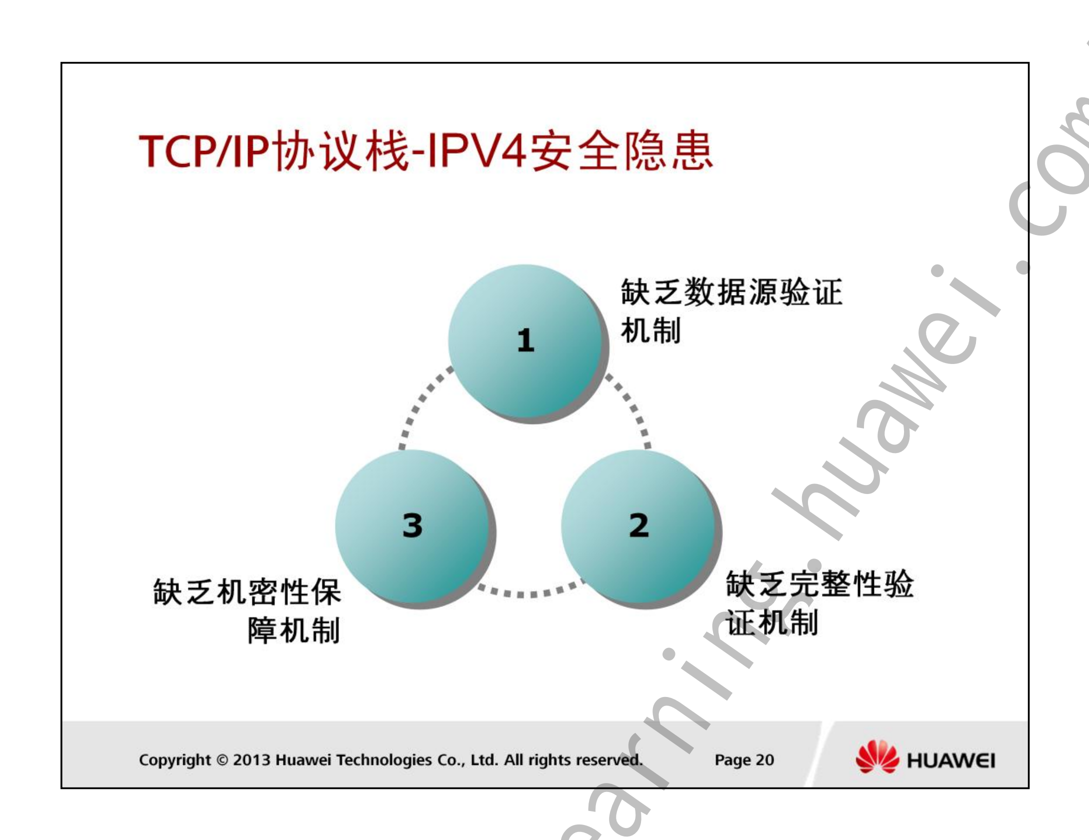
TCP终止连接的四次握手过程如下：

1. 首先进行关闭的一方（即发送第一个FIN）将执行主动关闭，而另一方（收到这个FIN）执行被动关闭。
2. 当服务器收到这个FIN，它发回一个ACK，确认序号为收到的序号加1。和SYN一样，一个FIN将占用一个序号。
3. 同时TCP服务器还向应用程序（即丢弃服务器）传送一个文件结束符。接着这个服务器程序就关闭它的连接，导致它的TCP端发送一个FIN。
4. 客户必须发回一个确认，并将确认序号设置为收到序号加1。



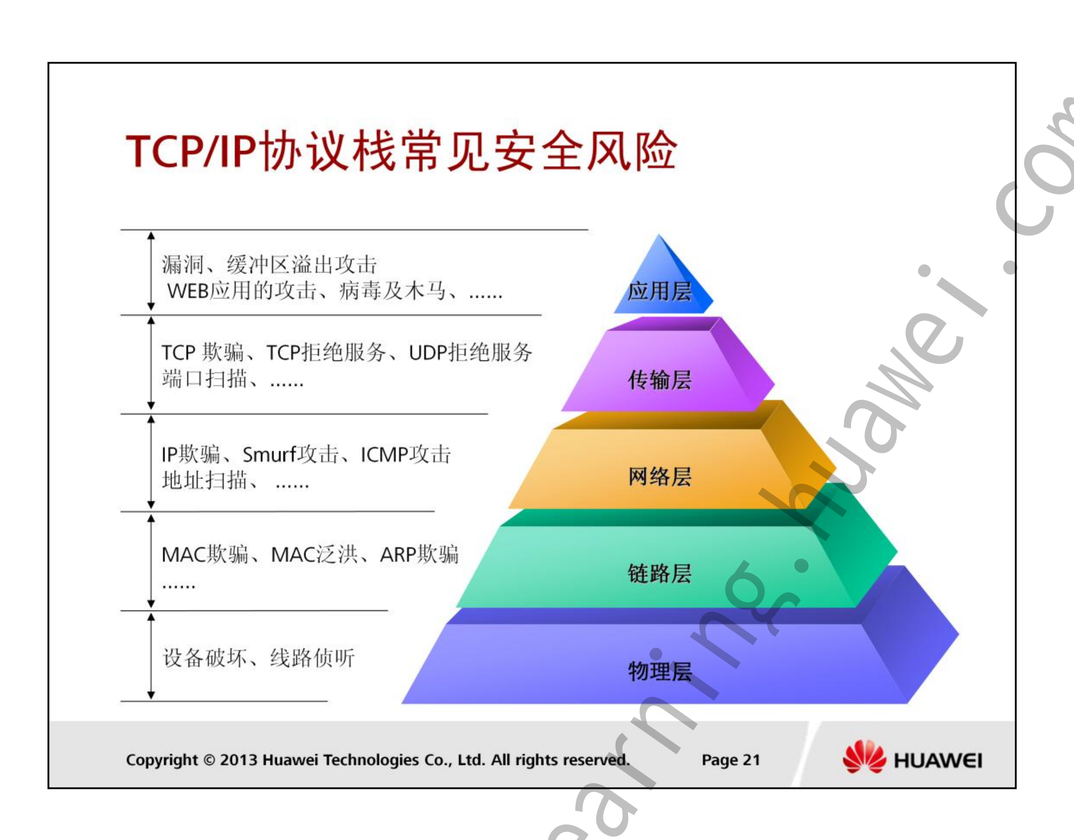
目录





随着互联网的不断发展，TCP/IP协议族成为使用最广泛的网络互连协议。但由于协议在设计之初对安全考虑的不够，导致协议存在着一些安全风险问题。Internet首先应用于研究环境，针对少量、可信的的用户群体，网络安全问题不是主要的考虑因素。因此，在TCP/IP协议栈中，绝大多数协议没有提供必要的安全机制，例如：

- 不提供认证服务
- 明码传输，不提供保密性服务，不提供数据保密性服务
- 不提供数据完整性保护
- 不提供抗抵赖服务
- 不保证可用性——服务质量（QoS）



TCP/IP协议栈中各层都有自己的协议。由于这些协议在开发之初并未重点考虑安全因素，缺乏必要的安全机制。因此，针对这些协议的安全威胁及攻击行为越来越频繁，TCP/IP协议栈的安全问题也越来越凸显。

设备破坏

- 物理设备破坏
  - 指攻击者直接破坏网络的各种物理设施，比如服务器设施，或者网络的传输通信设施等
  - 设备破坏攻击的目的主要是为了中断网络服务
- 设备破坏攻击防范
  - 主要靠非技术方面的因素，比如建造坚固的机房，指定严格的安全管理制度，对于需要铺设在外部环境中的通信电缆等，采用各种加强保护措施及安全管理措施



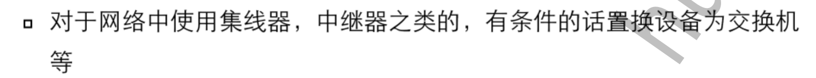
 Page 22 HUAWEI

设备破坏攻击一般不会容易造成信息的泄密，但通常会造成网络通信服务的中断，通常是一种暴力的攻击手段。

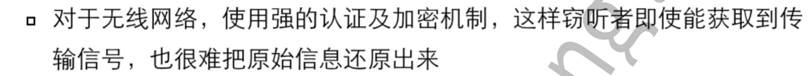
在日益强调网络服务的高可靠性的今天，设备破坏攻击是需要重点关注的。当然即使不是人为的故意破坏，针对各种自然条件下的物理损坏也是需要考虑的，比如中美海底通信光缆的被渔船挂断事故，台湾地震导致的海底光缆中断事故等。

线路侦听

- 物理层网络设备
  - 集线器
  - 中继器
- 无线网络
- 对线路侦听的防范



  - 对于网络中使用集线器，中继器之类的，有条件的话置换设备为交换机等



  - 对于无线网络，使用强的认证及加密机制，这样窃听者即使能获取到传输信号，也很难把原始信息还原出来

 Page 23



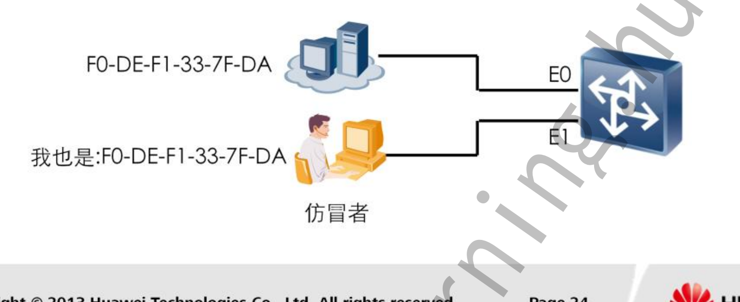
在常用网络设备中，集线器和中继器工作原理类似，从任何一个端口收上来的数据包都会转发到其它端口，这样，如果攻击者主机如果能够和这设备相连，通过相关的嗅探工具，就能够获取该网络上所有的通信数据信息。

对于无线网络，由于数据信息由无线信号传输，窃听者很容易获取到传输信号。

侦听在以太网组网中惯常使用，是基于传送进行攻击的基础。发起攻击的主机使用置于混杂模式的网卡，可以监听到同一物理网段内所有的报文。使用明文方式进行验证的协议，用户名和口令会泄露（SNMP/POP3/Telnet/..），使用明文进行传送的报文内容会泄漏；报文头中的内容也可能被利用。

MAC欺骗

- MAC欺骗是一种非常直观的攻击，攻击者将自己的MAC地址更改为受信任系统的地址。
- 对于MAC攻击的防范措施
  - 在交换机上配置静态条目，将特定的MAC地址始终与特定的端口绑定



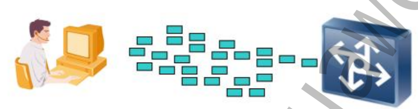
 Page 24 

针对交换机的Mac地址学习机制，攻击者通过伪造的源Mac地址数据包发送给交换机，造成交换机学习到了错误的Mac地址与端口的映射关系，导致交换机要发送到正确目的地的数据包被发送到了攻击者的主机上，攻击者主机通过安装相关的嗅探软件，可获得相关的信息以实现进一步的攻击。

通过在交换机上配置静态条目，绑定到正确的出接口，就能避免Mac欺骗攻击风险。

MAC泛洪

- MAC泛洪攻击利用了：
  - 交换机的MAC学习机制
  - MAC表项的数目限制
  - 交换机的转发机制
- MAC泛洪攻击的预防
  - 配置静态MAC转发表
  - 配置端口的MAC学习数目限制



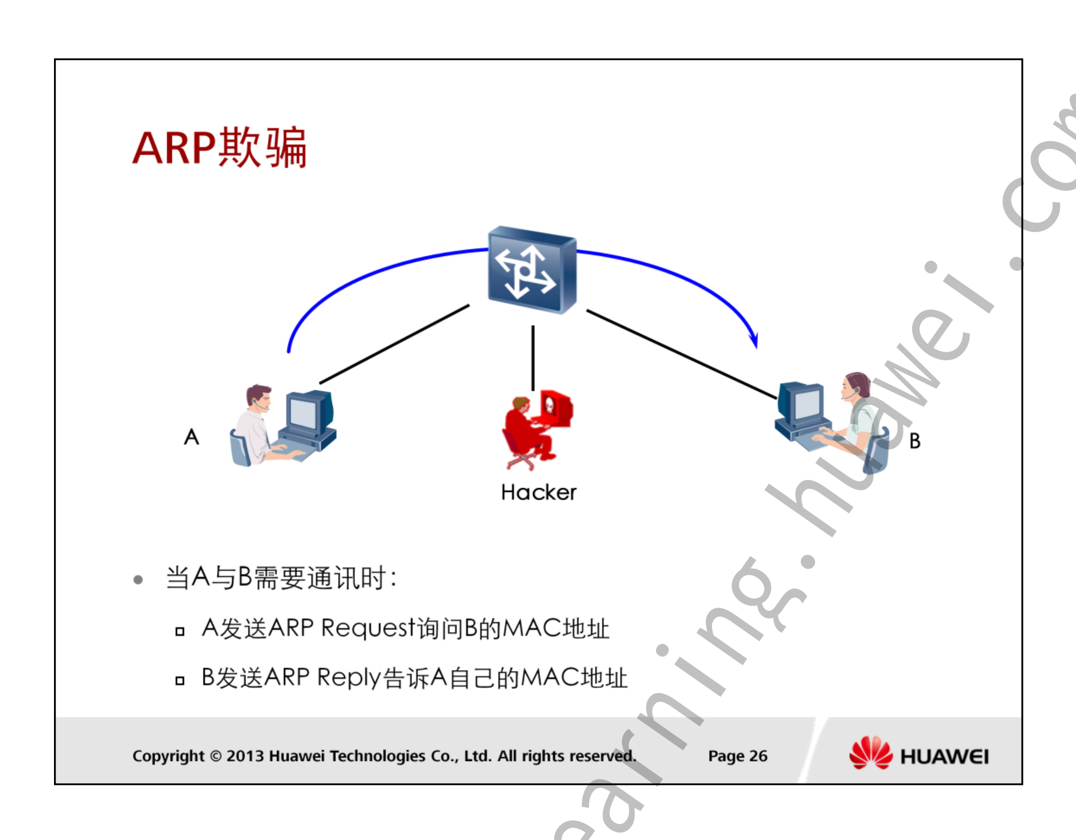
 Page 25



交换机比集线器的安全性更高的原因是交换机中的通信只在对应的端口之间，其它端口不能获取到该通信信息，降低了报文被侦听的风险。为了突破交换机的这种安全特性，结合交换机的工作特性，产生了Mac泛洪攻击，Mac泛洪攻击的直接后果一是交换机的转发性能大幅下降，二是交换机转发类似于集线器了，数据包在VLAN内的所有端口间泛洪。

Mac泛洪攻击一利用了交换机的Mac学习机制，攻击者通过发送伪造源地址的数据包，让交换机学习到错误的Mac转发表项，同时交换机的Mac表项是有一定数目限制的，通过发送大量的这种虚假信息包，交换机的Mac转发表项就会被这种虚假的信息占满，导致正常的数据包转发时匹配不到转发表项而泛洪到VLAN内的所有其它端口，这样就可以实现报文侦听了。

通过配置静态条目或者限制每端口的Mac地址学习数目来降低Mac泛洪攻击的风险。

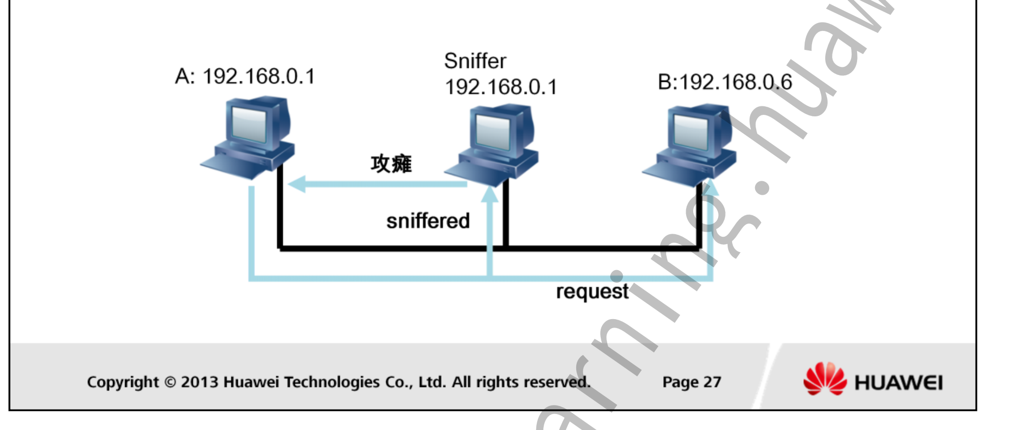


前面讲到MAC泛洪，使用这个方法会为网络带来大量垃圾数据报文，对于监听者来说也不是什么好事，很容易被发现，而且设计了端口保护的交换机可能会在超负荷时强行关闭所有端口造成网络中断。所以现在攻击者都偏向于使用地址解析协议ARP进行的欺骗性攻击。

ARP实现机制只考虑业务的正常交互，对非正常业务交互或恶意行为不做任何验证。比如当主机收到ARP响应包后，它并不会去验证自己是否发送过这个ARP请求，而是直接将应答包里的MAC地址与IP对应的关系替换掉原有的ARP缓存表。

在网络监听过程中，攻击者抢先合法主机B应答主机A发起的ARP请求；主机A被误导建立一个错误的映射并保存一段时间，在这段时间内，主机A发送给主机B的信息被误导致攻击者。如果攻击者持续抢先应答ARP请求，数据流就可能被一直误导下去。如果攻击者模拟网络出口路由器发动ARP攻击，内部网络的所有出口信息都将被接管。如果攻击者将出口路由器IP和一个不存在的MAC地址进行映射，即可以导致发送方受到拒绝服务的攻击。

ARP欺骗不仅仅可以通过ARP请求来实现，通过ARP响应也可以实现。



IP欺骗是利用了主机之间的正常信任关系来发动的。基于IP地址的信任关系的主机之间将允许以IP地址为基础的验证，允许或者拒绝以IP地址为基础的存取服务。信任主机之间无需输入口令验证就可以直接登录。

- IP欺骗攻击的整个步骤：

  （1）首先使被信任主机的网络暂时瘫痪，以免对攻击造成干扰；

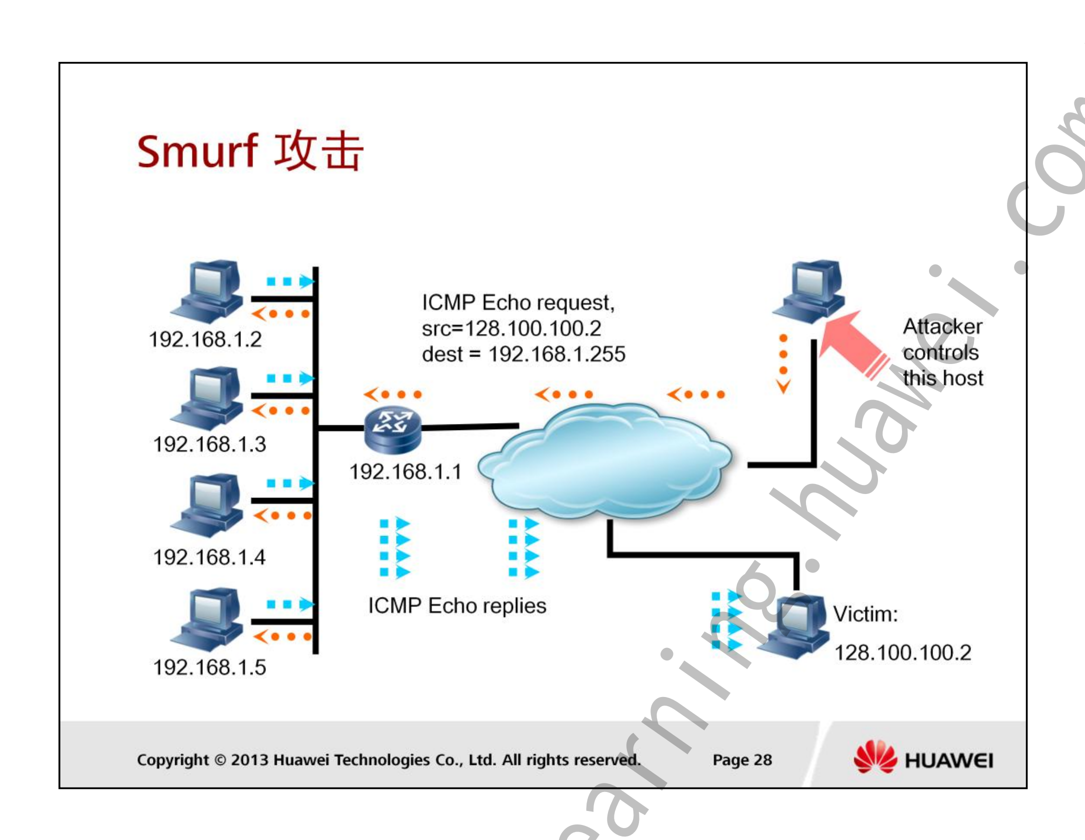
  （2）然后连接到目标机的某个端口来猜测序列号和增加规律；

  （3）接下来把源址址伪装成被信任主机，发送带有SYN标志的数据段请求连接；

  （4）然后等待目标机发送SYN+ACK包给已经瘫痪的主机；

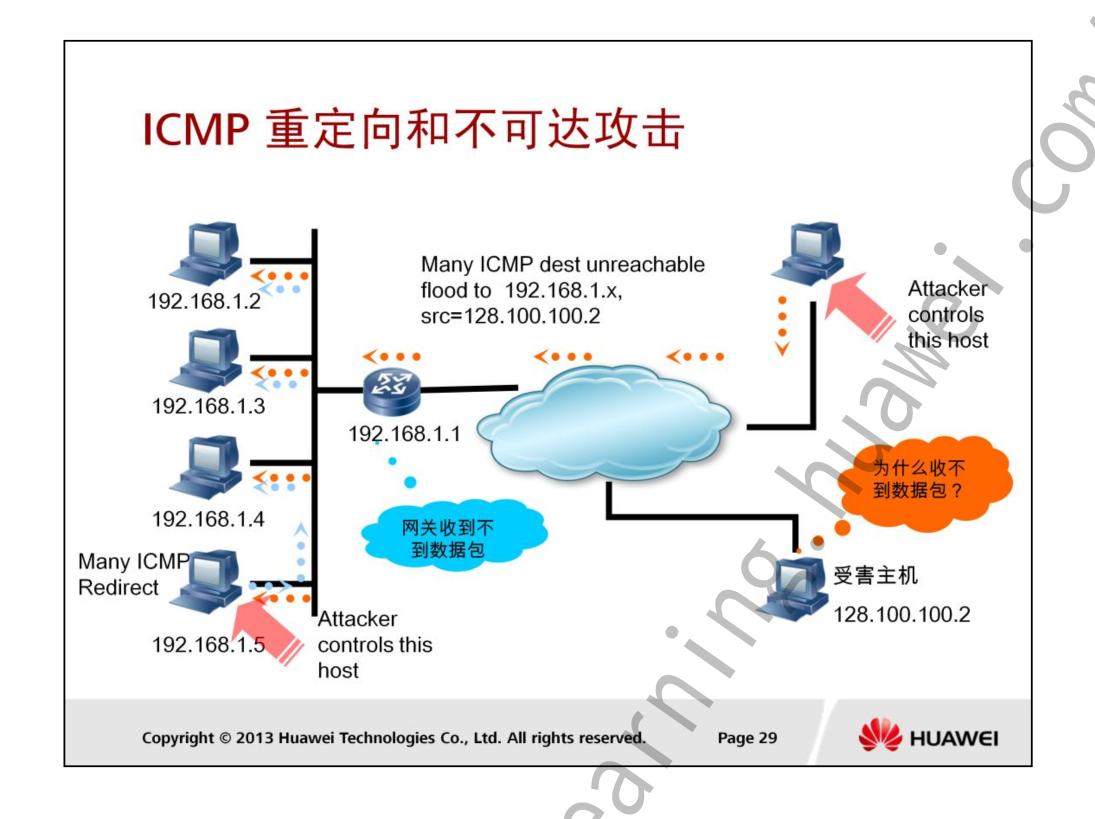
  （5）最后再次伪装成被信任主机向目标机发送的ACK，此时发送的数据段带有预测的目标机的序列号+1；

  （6）连接建立，发送命令请求。



Smurf攻击方法是发ICMP应答请求，该请求包的目标地址设置为受害网络的广播地址，这样该网络的所有主机都对此ICMP应答请求作出答复，导致网络阻塞。高级的Smurf攻击，主要用来攻击目标主机。方法是将上述ICMP应答请求包的源地址改为受害主机的地址，最终导致受害主机雪崩。攻击报文的发送需要一定的流量和持续时间，才能真正构成攻击。理论上讲，网络的主机越多，攻击的效果越明显。

针对Smurf攻击，在路由设备上配置检查ICMP应答请求包的目的地址是否为子网广播地址或子网的网络地址，如果是，则直接拒绝。



- ICMP重定向

ICMP重定向报文是ICMP控制报文中的一种。在特定的情况下，当路由器检测到一台机器使用非优化路由的时候，它会向该主机发送一个ICMP重定向报文，请求主机改变路由，路由器也会把初始数据报向它的目的地转发。ICMP虽然不是路由协议，但是有时它也可以指导数据包的流向（使数据流向正确的网关）。ICMP协议通过ICMP重定向数据包（类型5、代码0：网络重定向）达到这个目的。

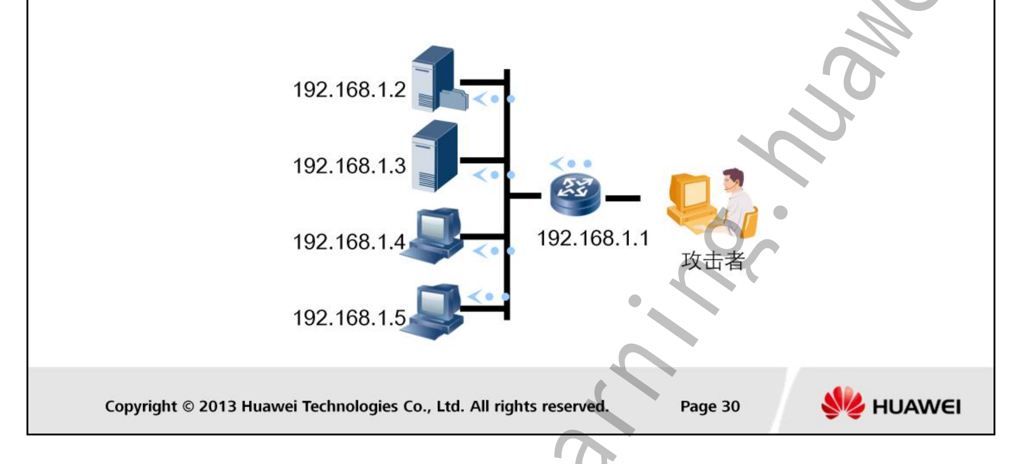
ICMP重定向攻击是攻击机主动向受害人主机发送ICMP重定向数据包，使受害人主机数据包发送到不正确的网关，达到攻击的目的。ICMP重定向攻击既可以从局域网内发起，也可以从广域网上发起。

针对ICMP重定向报文攻击，简单的办法就是通过修改注册表关闭主机的ICMP重定向报文处理功能。

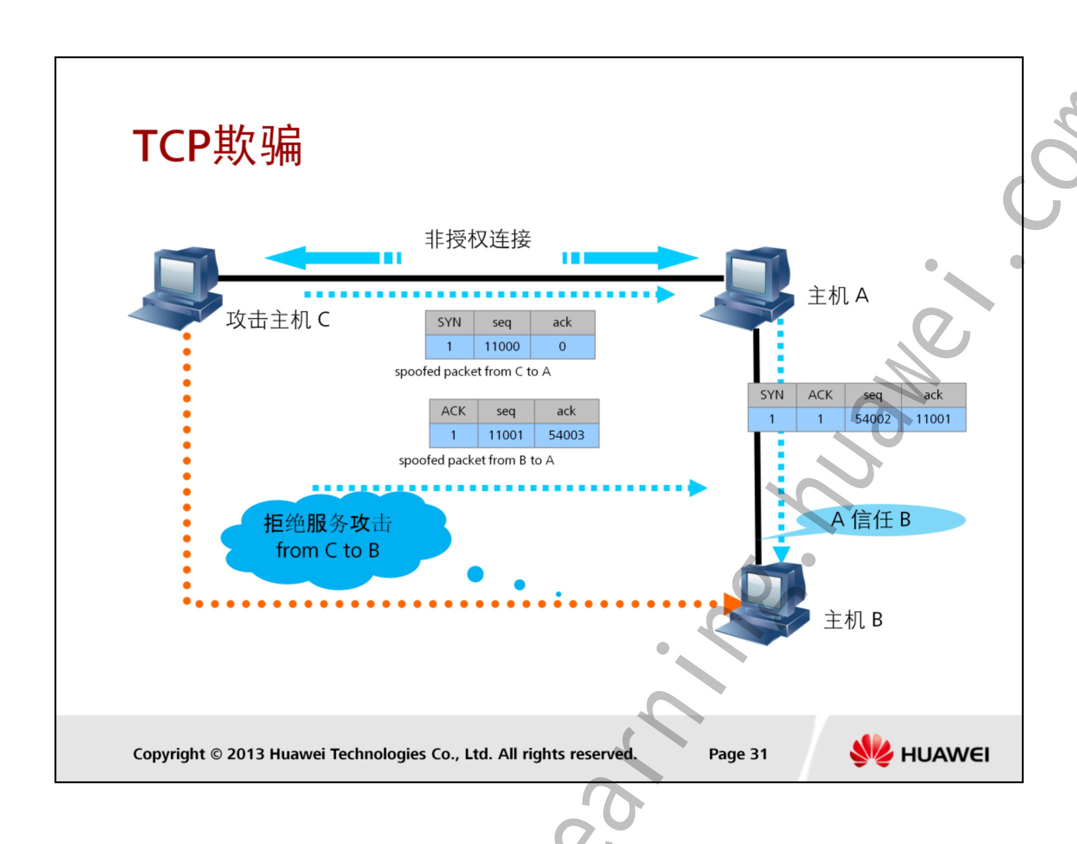
- ICMP不可达报文

不同的系统对ICMP不可达报文（类型为3）的处理不同，有的系统在收到网络（代码为0）或主机（代码为1）不可达的ICMP报文后，对于后续发往此目的地的报文直接认为不可达，好像切断了目的地与主机的连接，造成攻击。

针对ICMP不可达攻击，简单的办法就是通过修改注册表关闭主机的ICMP不可达报文处理功能。



IP地址扫描往往不是攻击者最终目的。攻击者通过IP地址扫描操作，获取目标网络的拓扑结构和存活的系统，为实施下一步攻击做准备。

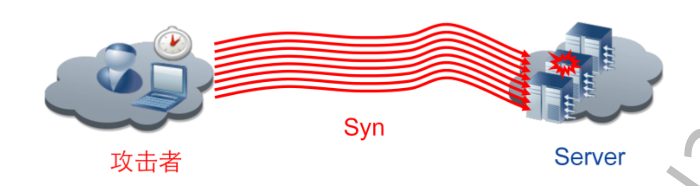


TCP欺骗大多数发生在TCP连接建立的过程中，利用主机之间某种网络服务的信任关系建立虚假的TCP连接，可能模拟受害者从服务器端获取信息。具体过程与IP欺骗类似。

例如：A信任B，C是攻击者，想模拟B和A之间建立连接。

1. C先破坏掉B，例如使用floogin, redirect, crashing等
2. C用B的地址作为源地址给A发送TCP SYN报文
3. A回应TCP SYN/ACK报文，从A发给B，携带序列码S
4. C收不到该序列码S，但为了完成握手必须用S+1作为序列码进行应答，这时C可以通过以下两种方法得到序列码S：
   - C 监听SYN/ACK报文，根据得到的值进行计算
   - C 根据A操作系统的特性等，进行猜测
5. C使用得到的序列码S回应A，握手完成，虚假连接建立…

TCP拒绝服务——SYN Flood攻击

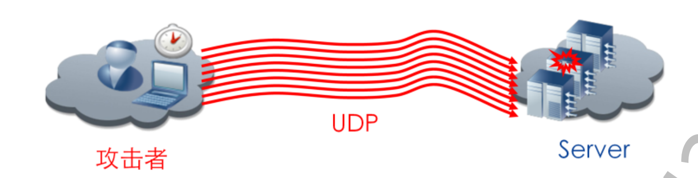


- SYN报文是TCP连接的第一个报文，攻击者通过大量发送SYN报文，造成大量未完全建立的TCP连接，占用被攻击者的资源。

 Page 32 

- SYN FLOODING攻击特点：
  - 攻击者用带有SYN标志位的数据片断启动握手
  - 受害者用SYN-ACK应答；
  - 攻击者保持沉默，不进行回应；
  - 由于主机只能支持数量有限的TCP连接处于half-open的状态，超过该数目后，新的连接就都会被拒绝；
- 目前的解决方法：关闭处于Half Open 状态的连接。

UDP拒绝服务——UDP Flood攻击



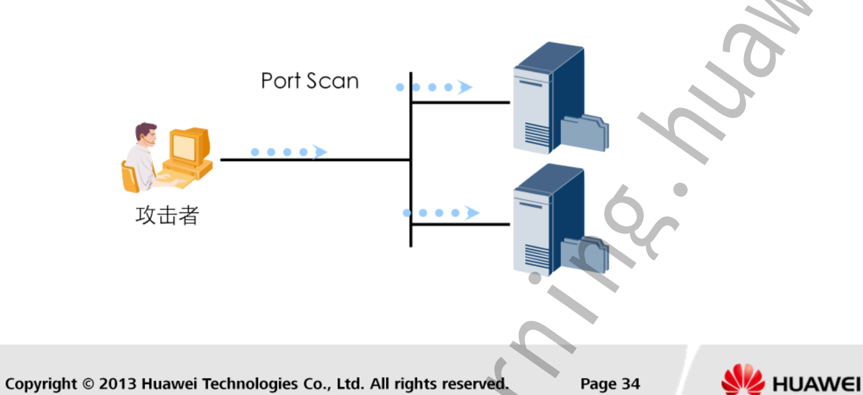
- 攻击者通过向服务器发送大量的UDP报文，占用服务器的链路带宽，导致服务器负担过重而不能正常向外提供服务。

Page 33



由于UDP协议是无连接的，所以不能对其进行连接状态的检测。通过对UDP报文进行主动统计和学习，分析某个主机发送UDP报文的规律和特征，如果存在一台主机大量发送相同、相似或以某种特定规律变化的UDP报文时，则将其认为是攻击者。

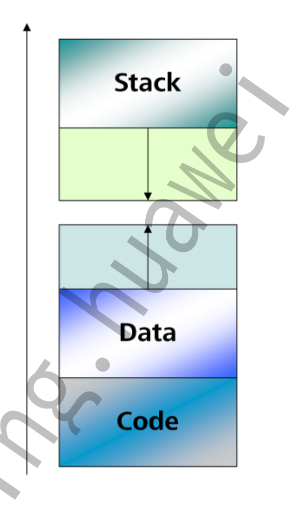
通过配置对UDP报文速率限制，可以实现UDP Flood的攻击防范。



配置端口扫描攻击防范参数后，设备对进入的TCP，UDP，ICMP报文进行检测，并以某个源IP地址为索引，判断该源IP地址发送报文的目的端口与前一报文的目的端口是否不同，如果是则异常次数加1。当异常频率超过预定义的阈值时，则认为该源IP地址的报文为端口扫描攻击，并将该源IP地址加入黑名单。

缓冲区溢出攻击

- 攻击软件系统的行为中，最常见的一种方法
- 可以从本地实施，也可以从远端实施
- 利用软件系统（操作系统，网络服务，程序库）实现中对内存操作的缺陷，以高操作权限运行攻击代码
- 漏洞与操作系统和体系结构相关，需要攻击者有较高的知识/技巧





缓冲区是内存中存放数据的地方。在程序试图将数据放到机器内存中的某一个位置的时候，因为没有足够的空间就会发生缓冲区溢出。而人为的溢出则是有一定企图的，攻击者写一个超过缓冲区长度的字符串，植入到缓冲区，然后再向一个有限空间的缓冲区中植入超长的字符串，这时可能会出现两个结果：一是过长的字符串覆盖了相邻的存储单元，引起程序运行失败，严重的可导致系统崩溃；另一个结果就是利用这种漏洞可以执行任意指令，甚至可以取得系统root特级权限。

针对WEB应用的攻击

- 常见的攻击
  - 对客户端的
    - 含有恶意代码的网页，利用浏览器的漏洞，威胁本地系统
  - 对Web服务器的
    - 利用Apache/IIS…的漏洞
    - 利用CGI实现语言(PHP/ASP/Perl...)和实现流程的漏洞
  - 通过Web服务器，入侵数据库

 Page 36



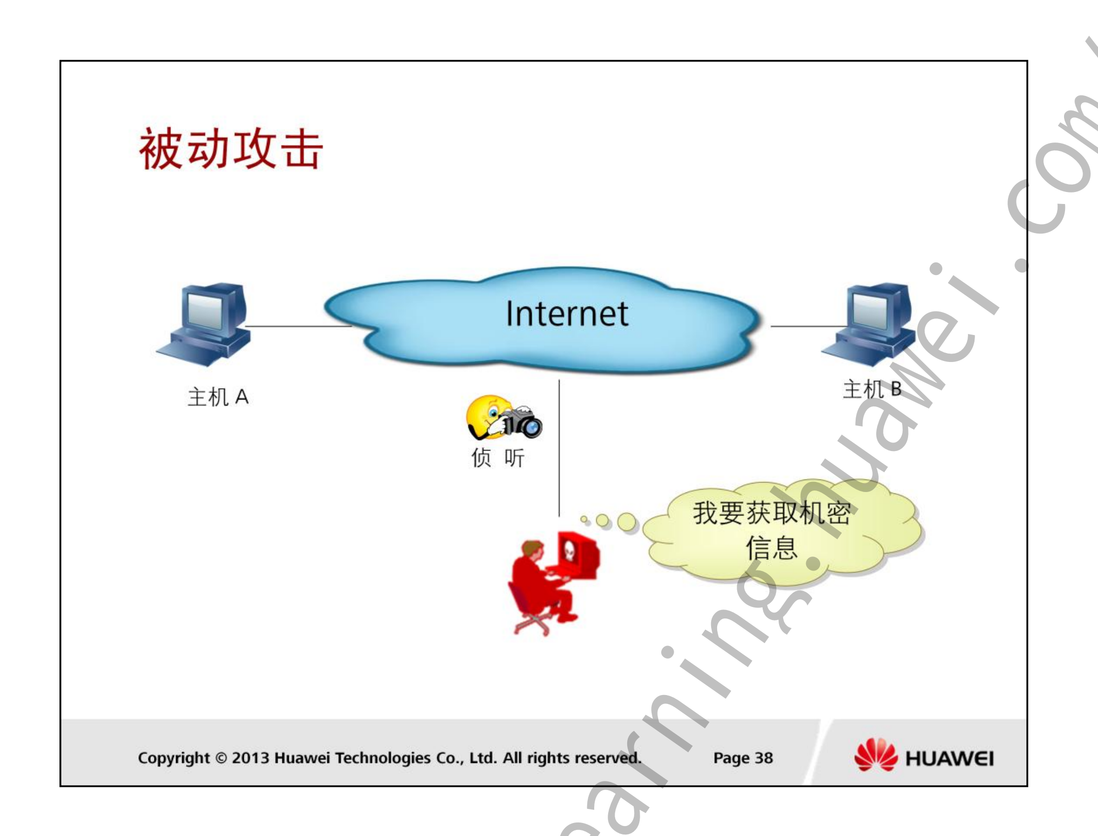
典型的WEB应用由三层构成:

- 客户端 – 浏览器/Javasrcipt/Applet
- 表现层 – HTTP Server + Server Side script
- 业务逻辑和数据存储层 – 业务逻辑的实现和数据库



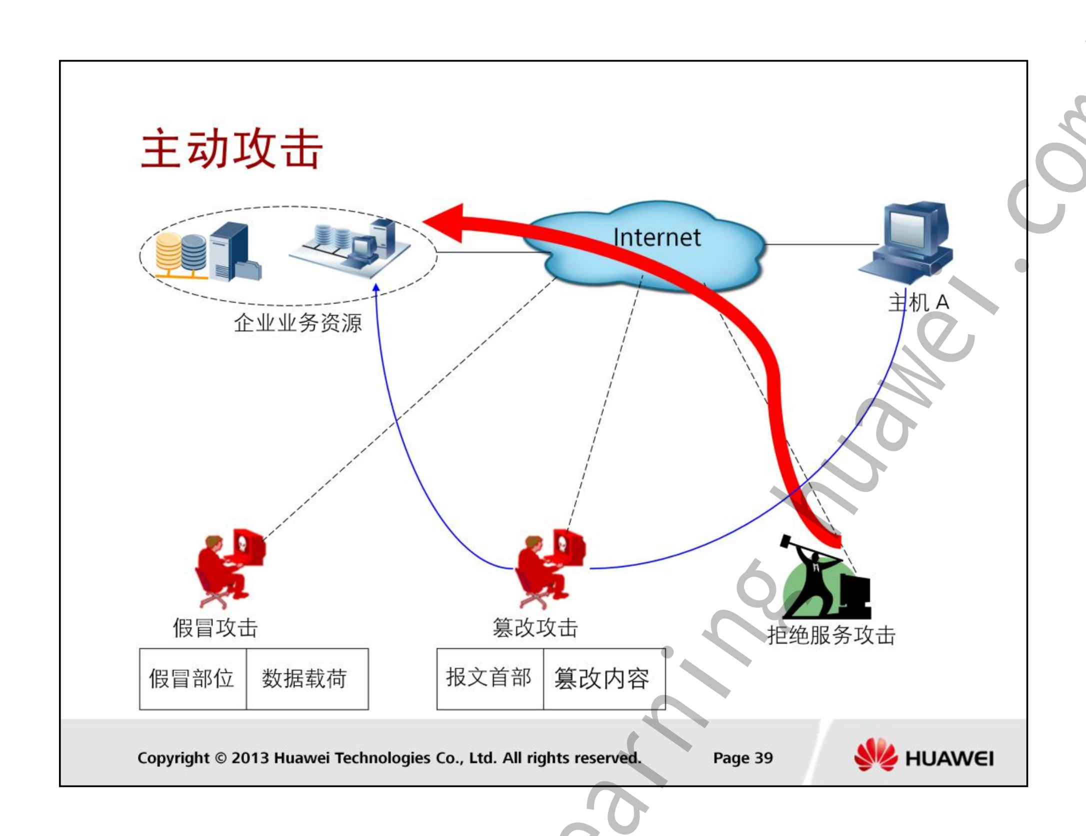
目录



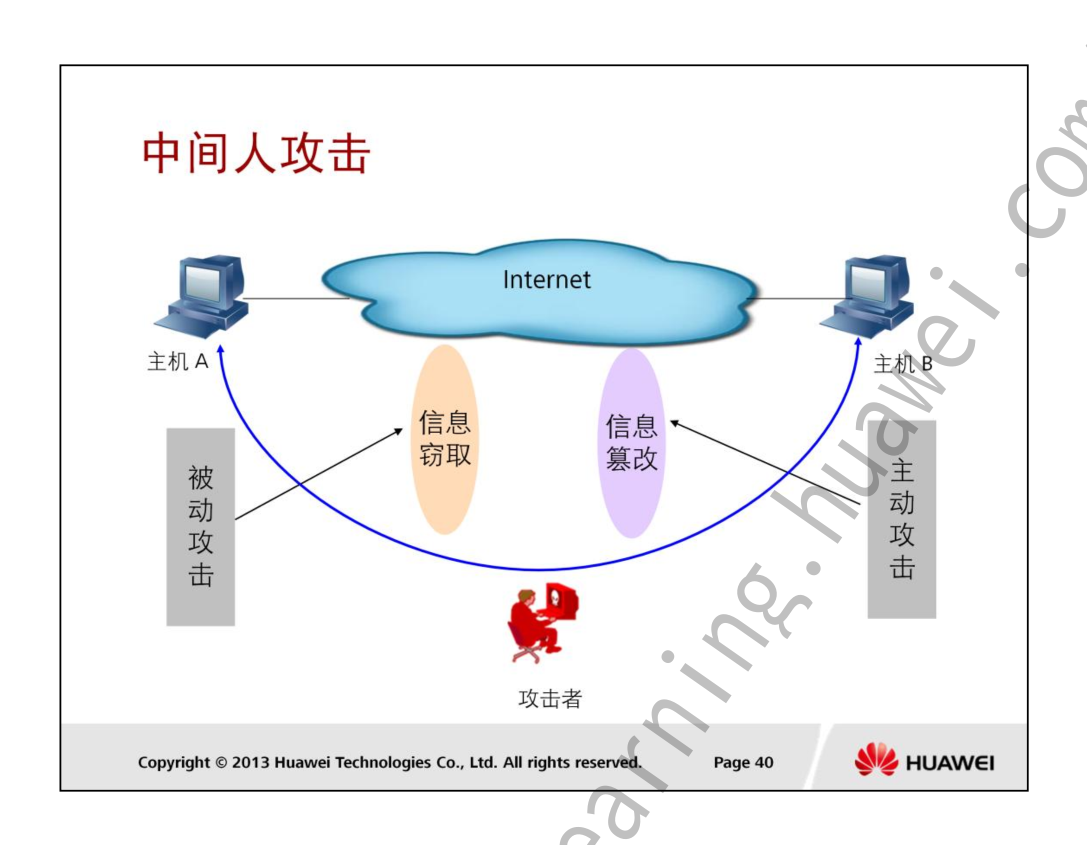


被动攻击最大特点是对想窃取信息进行侦听，以获取机密信息。而对数据的拥有者或合法用户来说，对此类活动无法得知，所以被动攻击主要关注防范，而非检测。

目前针对此类攻击行为，一般都是采用加密技术来保护信息的机密性。



主动攻击主要包括对业务数据流报文首部或数据载荷部分进行假冒或篡改，以达到冒充合法用户对业务资源进行非授权访问，或对业务资源进行破坏性攻击。对于此类攻击可通过对数据流进行分析检测以给出技术解决措施，最终保障业务的正常运行。比如数据源验证、完整性验证、防拒绝攻击技术等。



中间人攻击是一种“间接”类型的攻击方式，根据攻击者对信息的不同攻击行为（信息窃取攻击、信息篡改攻击），将会有被动攻击和主动攻击的特征。

- 信息窃取：

当主机A和主机B进行数据交互时，攻击者对信息进行截取备份一份，并进行数据转发（可能只是进行侦听，不对其进行转发）。这样攻击者很容易获取主机A和主机B机密信息，而主机A和主机B对其一无所知；

- 信息篡改：

攻击者做为主机A和主机B数据交互的中介，可能对主机A和主机B来看以为他们之间是直接通信，其实他们之间通讯有个中转器-攻击者。此类攻击，攻击者一般会往主机A和主机B之间数据流中插入或更改相应信息，以达到其攻击的目标。

针对以上攻击方式，对于攻击来说，一般会采用各类技术以达到信息截取的目标，比如DNS欺骗、网络流侦听等。



总结

- OSI模型
- TCP/IP协议原理
- TCP/IP协议存在的安全问题
- 针对TCP/IP各层的常见攻击



思考题

- 为什么ARP欺骗攻击容易实现?
- 如何实现IP欺骗攻击?
- TCP协议与UDP协议有何区别?
- 为什么TCP建立连接是三次握手，而断开连接是四次握手?



Thank you

www.huawei.com

HC110310002

HCNA-Security-CBSN 第二章 防火墙基础技术


第二章
防火墙基础技术
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目标

- 学完本课程后，您将能够:
  - 了解防火墙的定义和分类
  - 理解防火墙的主要功能和技术
  - 掌握防火墙设备管理的方法
  - 掌握防火墙的基本配置





目录



防火墙特征

- 逻辑区域过滤器
- 隐藏内网网络结构
- 自身安全保障
- 主动防御攻击

被入侵
内网
防火墙
Internet
路由器
未经防火墙流量可防护吗?

 Page 3 HUAWEI

防火墙技术是安全技术中的一个具体体现。防火墙原本是指房屋之间修建的一道墙，用以防止火灾发生时的火势蔓延。我们这里讨论的是硬件防火墙，它是将各种安全技术融合在一起，采用专用的硬件结构，选用高速的CPU、嵌入式的操作系统，支持各种高速接口（LAN接口），用来保护私有网络（计算机）的安全，这样的设备我们称为硬件防火墙。硬件防火墙可以独立于操作系统（HP-UNIX、SUN OS、AIX、NT等）、计算机设备（IBM6000、普通PC等）运行。它用来集中解决网络安全问题，可以适合各种场合，同时能够提供高效率的“过滤”。同时它可以提供包括访问控制、身份验证、数据加密、VPN技术、地址转换等安全特性，用户可以根据自己的网络环境的需要配置复杂的安全策略，阻止一些非法的访问，保护自己的网络安全。

现代的防火墙体系不应该只是一个“入口的屏障”，防火墙应该是几个网络的接入控制点，所有进出被防火墙保护的网络的数据流都应该首先经过防火墙，形成一个信息进出的关口，因此防火墙不但可以保护内部网络在Internet中的安全，同时可以保护若干主机在一个内部网络中的安全。在每一个被防火墙分割的网络内部中，所有的计算机之间是被认为“可信任的”，它们之间的通信不受防火墙的干涉。而在各个被防火墙分割的网络之间，必须按照防火墙规定的“策略”进行访问。

防火墙分类

- 按照形态分为
  - 硬件防火墙
  - 软件防火墙
- 按照保护对象分为
  - 单机防火墙
  - 网络防火墙
- 按照访问控制方式分为
  - 包过滤防火墙
  - 代理防火墙
  - 状态检测防火墙

 Page 4 

防火墙发展至今已经历经三代，分类方法也各式各样，例如按照形态划分可以分为硬件防火墙及软件防火墙；按照保护对象划分可以分为单机防火墙及网络防火墙等。但总的来说，最主流的划分方法是按照访问控制方式进行分类。

网络防火墙，能够分布式保护整个网络，其特点：

1）安全策略集中；

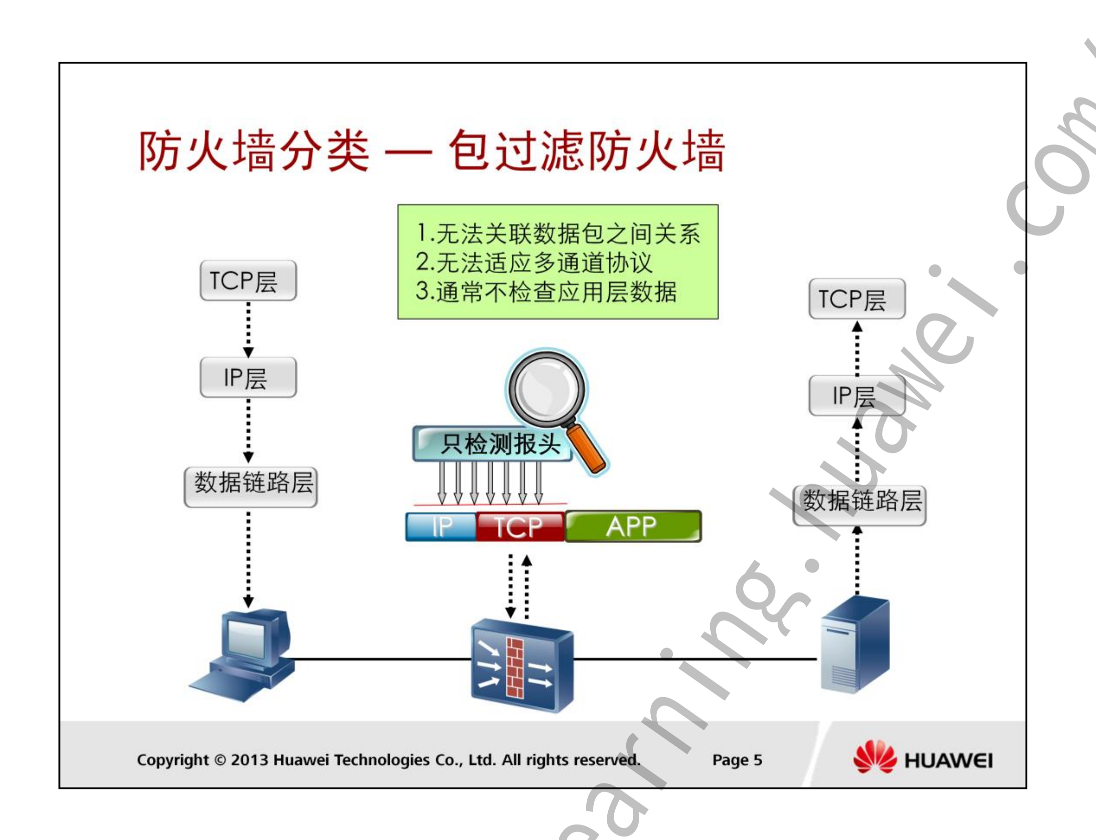
2）安全功能复杂多样；

3）专业管理员维护；

4）安全隐患小；

5）策略设置复杂。

本课程重点介绍按照访问控制方式分类。



包过滤是指在网络层对每一个数据包进行检查，根据配置的安全策略转发或丢弃数据包。包过滤防火墙的基本原理是：通过配置访问控制列表（ACL, Access Control List）实施数据包的过滤。主要基于数据包中的源/目的IP地址、源/目的端口号、IP 标识和报文传递的方向等信息。

包过滤防火墙的设计简单，非常易于实现，而且价格便宜。

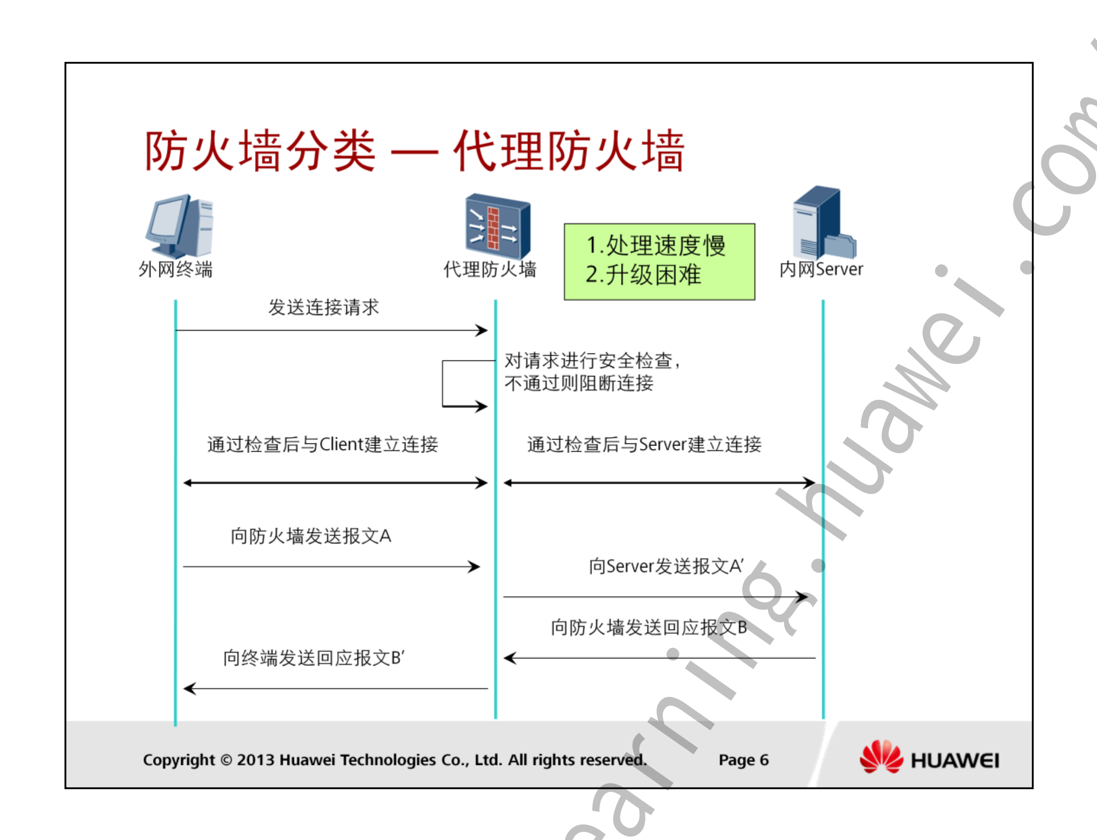
包过滤防火墙的缺点主要表现以下几点：

1. 随着ACL 复杂度和长度的增加，其过滤性能呈指数下降趋势。

2. 静态的ACL 规则难以适应动态的安全要求。

3. 包过滤不检查会话状态也不分析数据，这很容易让黑客蒙混过关。例如，攻击者可以使用假冒地址进行欺骗，通过把自己主机IP地址设成一个合法主机IP地址，就能很轻易地通过报文过滤器。

说明：多通道协议，如FTP协议。FTP在控制通道协商的基础上，生成动态的数据通道端口，而后的数据交互主要在数据通道上进行。

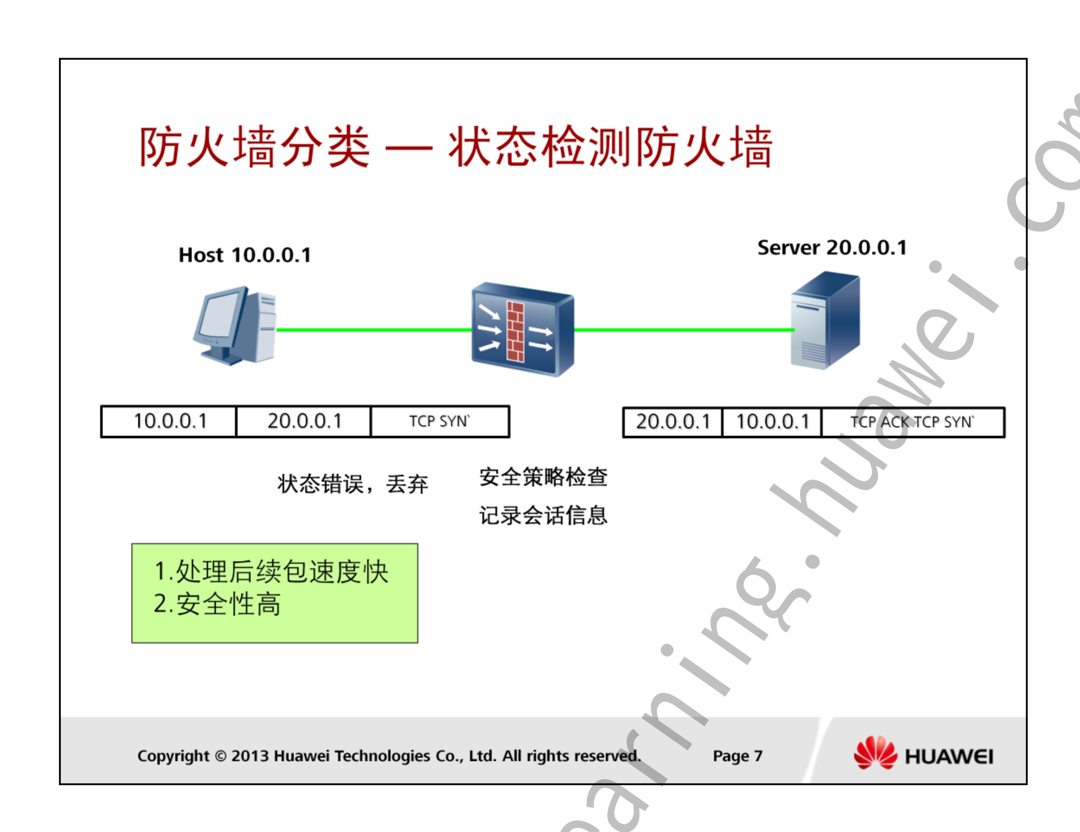


代理服务作用于网络的应用层，其实质是把内部网络和外部网络用户之间直接进行的业务由代理接管。代理检查来自用户的请求，用户通过安全策略检查后，该防火墙将代表外部用户与真正的服务器建立连接，转发外部用户请求，并将真正服务器返回的响应回送给外部用户。

代理防火墙能够完全控制网络信息的交换，控制会话过程，具有较高的安全性。其缺点主要表现在：

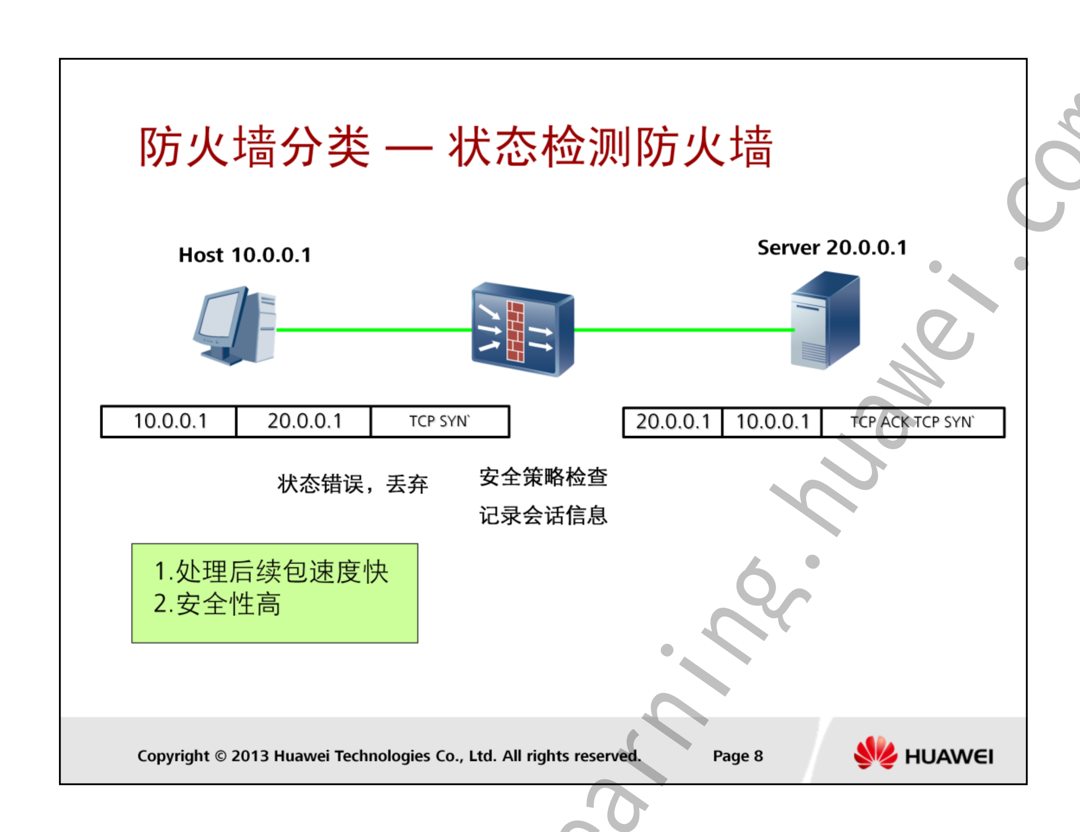
1. 软件实现限制了处理速度，易于遭受拒绝服务攻击。

2. 需要针对每一种协议开发应用层代理，开发周期长，而且升级很困难。

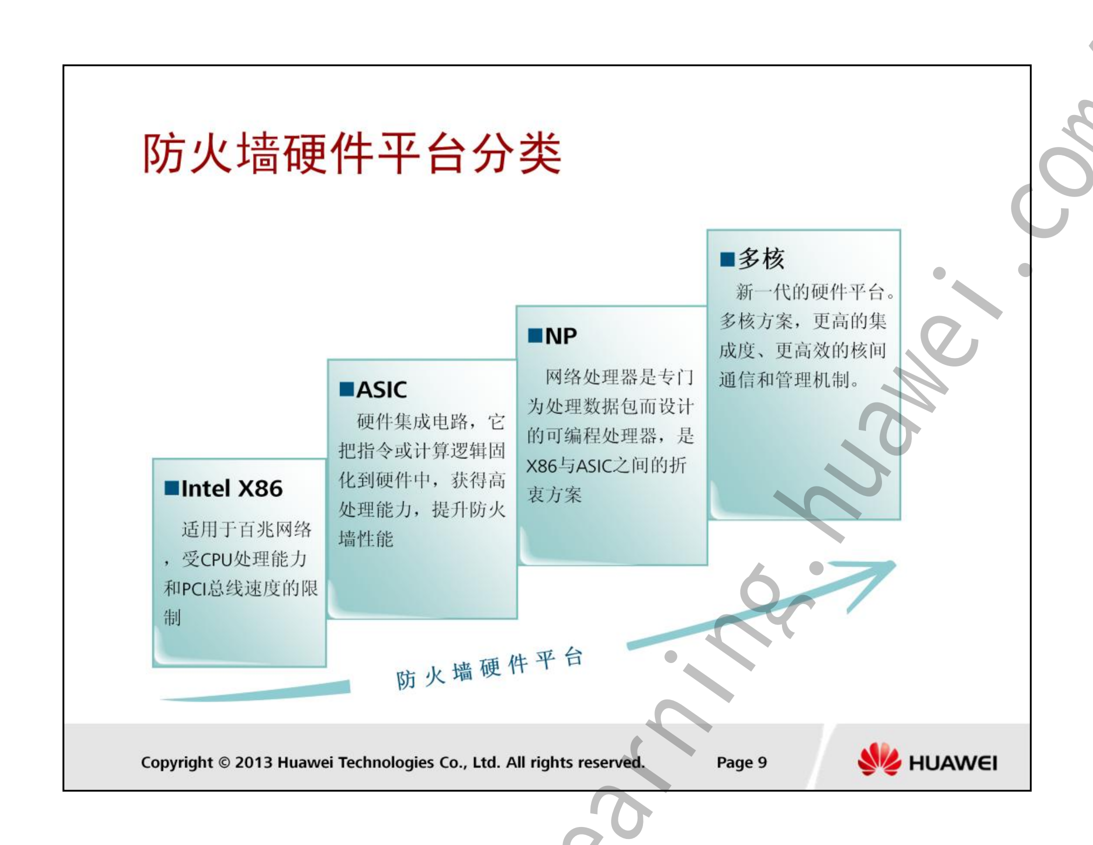


状态检测是包过滤技术的扩展。基于连接状态的包过滤在进行数据包的检查时，不仅将每个数据包看成是独立单元，还要考虑前后报文的历史关联性。我们知道，所有基于可靠连接的数据流（即基于TCP协议的数据流）的建立都需要经过“客户端同步请求”、“服务器应答”以及“客户端再应答”三个过程（即“三次握手”过程），这说明每个数据包都不是独立存在的，而是前后有着密切的状态联系的。基于这种状态联系，从而发展出状态检测技术。

- 基本原理简述如下：
  - 状态检测防火墙使用各种会话表来追踪激活的TCP（Transmission Control Protocol）会话和UDP（User Datagram Protocol）伪会话，由访问控制列表决定建立哪些会话，数据包只有与会话相关联时才会被转发。其中UDP伪会话是在处理UDP协议包时为该UDP数据流建立虚拟连接（UDP是面对无连接的协议），以对UDP 连接过程进行状态监控的会话。
  - 状态检测防火墙在网络层截获数据包，然后从各应用层提取出安全策略所需要的状态信息，并保存到会话表中，通过分析这些会话表和与该数据包有关的后续连接请求来做出恰当决定。



- 状态检测防火墙具有以下优点：
  - 后续数据包处理性能优异：状态检测防火墙对数据包进行ACL 检查的同时，可以将数据流连接状态记录下来，该数据流中的后续包则无需再进行ACL检查，只需根据会话表对新收到的报文进行连接记录检查即可。检查通过后，该连接状态记录将被刷新，从而避免重复检查具有相同连接状态的数据包。连接会话表里的记录可以随意排列，与记录固定排列的ACL 不同，于是状态检测防火墙可采用诸如二叉树或哈希（Hash）等算法进行快速搜索，提高了系统的传输效率。
  - 安全性较高：连接状态清单是动态管理的。会话完成后防火墙上所创建的临时返回报文入口随即关闭，保障了内部网络的实时安全。同时，状态检测防火墙采用实时连接状态监控技术，通过在会话表中识别诸如应答响应等连接状态因素，增强了系统的安全性。



防火墙的硬件平台发展至今，大致可以划分为通用CPU架构、专用集成电路（ASIC, Application Specific Integrated Circuit）架构、网络处理（NP, Network Processor）架构以及多核处理器架构。下面我们将一一进行介绍。

- **通用CPU架构**

通用CPU架构是基于X86平台，使用一颗主CPU来处理业务的架构。网卡芯片与CPU使用PCI总线进行数据的传输。传统32位PCI总线，网卡芯片与CPU之间的数据传输速率理论上可以达到1056Mbits/s，理论上满足千兆防火墙的需要。但是X86平台使用的是共享总线的一种架构，因此如果有两块网卡同时传输数据，则平均下来每块网卡只能获得528 Mbits/s的速率。网卡数量越多，获得的速率就越低，并且只要超过一块网卡，速率就低于1000Mbits/s。另外，基于X86平台的架构，其线程调度机制是采用中断方式来实现的，因此当网络中出现大量数据小包时，与大包相比，相同的流量将产生更多的中断，此时防火墙的吞吐量就只有20%左右，并且CPU占用率非常高。因此实际上这种基于X86平台的架构就无法满足千兆防火墙的需要，只适合作为百兆防火墙的硬件平台方案。

随着硬件技术的发展，后来Intel针对PCI总线提出一种新的解决方案——PCI-Express。PCI-E的主要优势就是数据传输速率高，目前最高可达到10GB/s以上。X86平台使用PCI-E技术后，数据传输速率已经可以满足千兆防火墙的要求，但是其中断机制对整机处理速率的影响仍然存在，因此X86采用PCI-E技术后仍有很大的问题需改进。

- **ASIC架构**

相比之下，基于ASIC架构的防火墙从架构上改进了中断机制。ASIC设计专门的ASIC芯片对数据进行加速处理，并且将指令以及算法直接固化到芯片中。数据从网卡收到以后，不经过主CPU处理，而是经过集成在网卡上的ASIC芯片，通过ASIC芯片直接对数据进行处理并转发。这样，数据就并非全部需要通过主CPU来处理，芯片处理也不采用中断机制，自然可以明显提高了防火墙的处理性能。

但ASIC也有它自己的短板，就是它的灵活性及扩展性非常差。ASIC架构毕竟采用的是芯片，然而芯片的开发非常困难，能够处理的业务也非常有限，面对应用较为复杂的网络时，ASIC架构明显无法胜任。

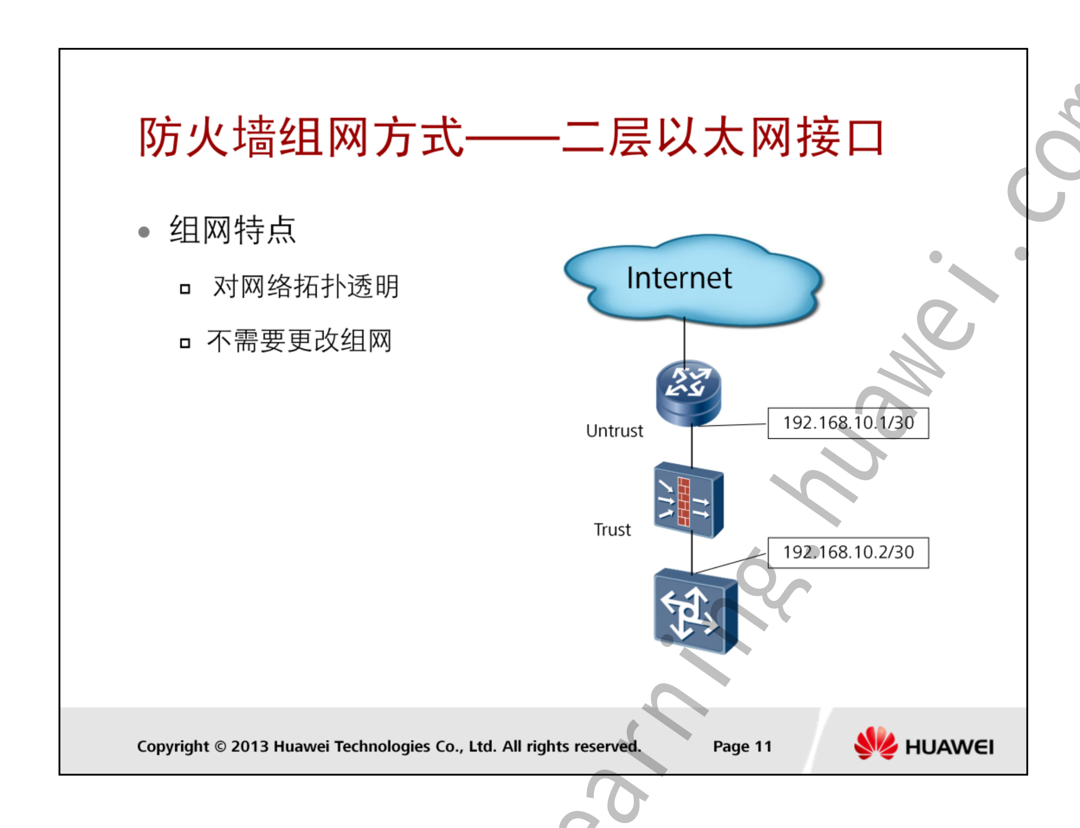
- **NP架构**

NP架构可以说是CPU方案与ASIC方案的一个折衷方案，它在每块网卡上使用了一个网络处理器。网络处理器是专门为网络设备处理网络流量而设计的处理器。NP与X86架构相比，在性能上有着明显的优势。但网络处理器微码编程还是不够灵活，功能的扩展仍然受到一定程度的限制；与ASIC相比，由于处理流程对软件一定程度上的依赖，因而转发性能也比ASIC稍弱。

- **多核架构**

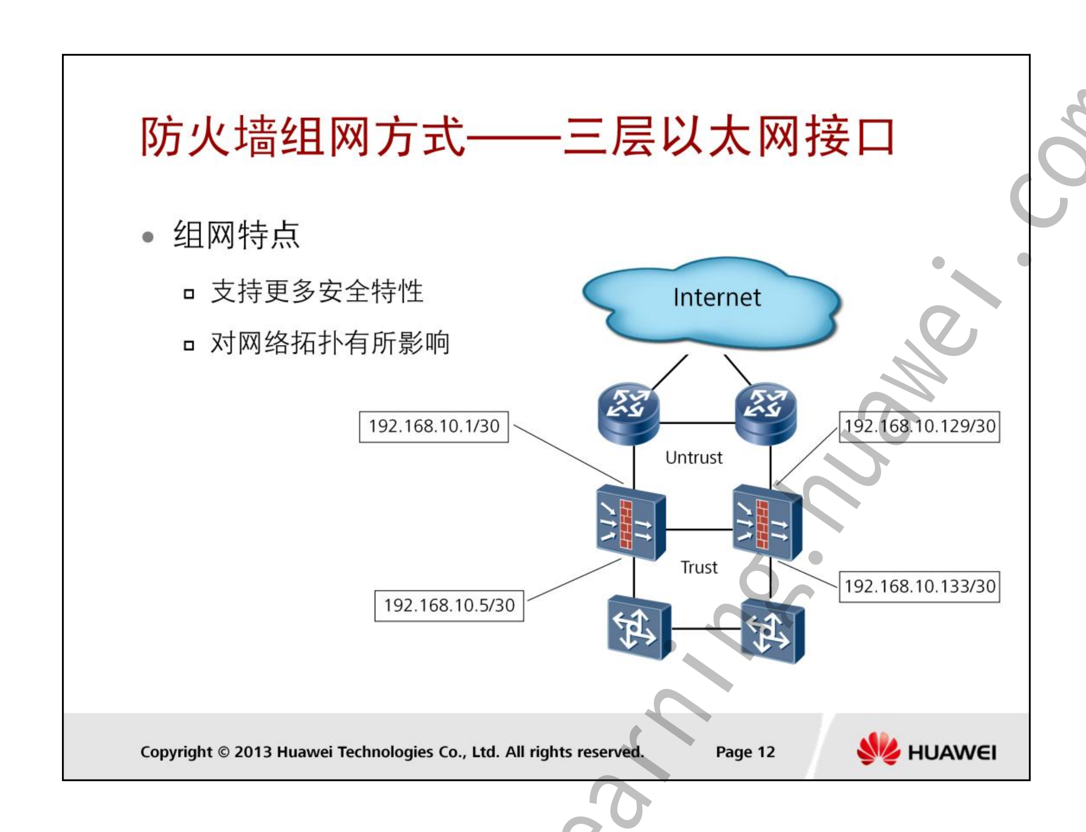
从上面可以看出，通用CPU架构、NP架构以及ASIC架构各有优缺点。多核架构的出现极大地缓和了这些矛盾。多核架构中每一个核都是一个通用CPU，相对于多CPU方案提供了更高的集成度、更高效的核间通信和管理机制。少量的核完成管理功能，大多数核完成例行的业务处理功能。有些CPU通过协处理器来实现加解密，而且由于可以采用c编程，功能扩展不受控制，平台可以实现VPN加解密、防火墙、UTM等业务而不影响相应性能。

多核作为新一代的硬件平台，对软件开发技术的要求非常高，如何有效实现和发挥多核技术的优势，是基于多核硬件平台进行产品开发的巨大挑战。对这种基于多核硬件平台的防火墙，华为防火墙融合了许多技术优势，更完美地利用多核技术，如多核操作系统SOS（Security Operation System）。多核处理器有强大的并行处理能力和I/O能力，硬件辅助数据报文调度能力，但是通用的操作系统在CPU内核数量增加的情况下，效率下降很快。SOS系统高效、稳定、安全，适合作为高性能网络转发、安全业务开发平台，支持高效的报文调度，并发处理，最大程度的提高多核CPU的利用率。



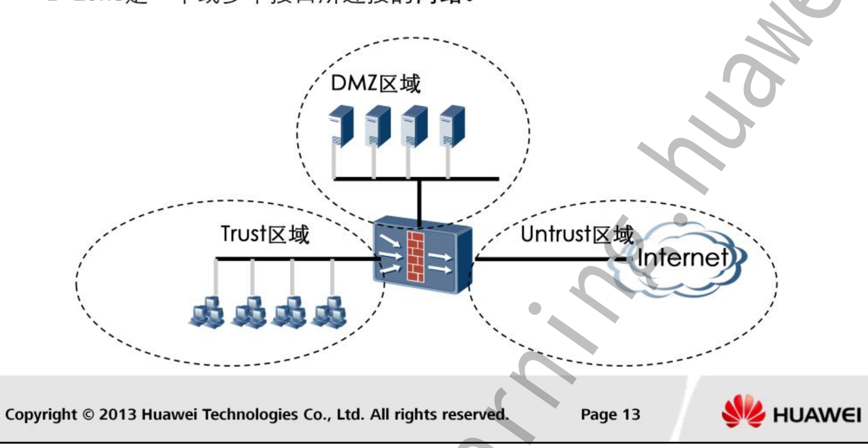
在此组网方式下，防火墙只进行报文转发，不能进行路由寻址，与防火墙相连两个业务网络必须在同一个网段中。此时防火墙上下行接口均工作在二层，接口无IP地址。

防火墙此组网方式可以避免改变拓扑结构造成的麻烦，只需在网络中像放置网桥（Bridge）一样串入防火墙即可，无需修改任何已有的配置。IP报文同样会经过相关的过滤检查，内部网络用户依旧受到防火墙的保护。

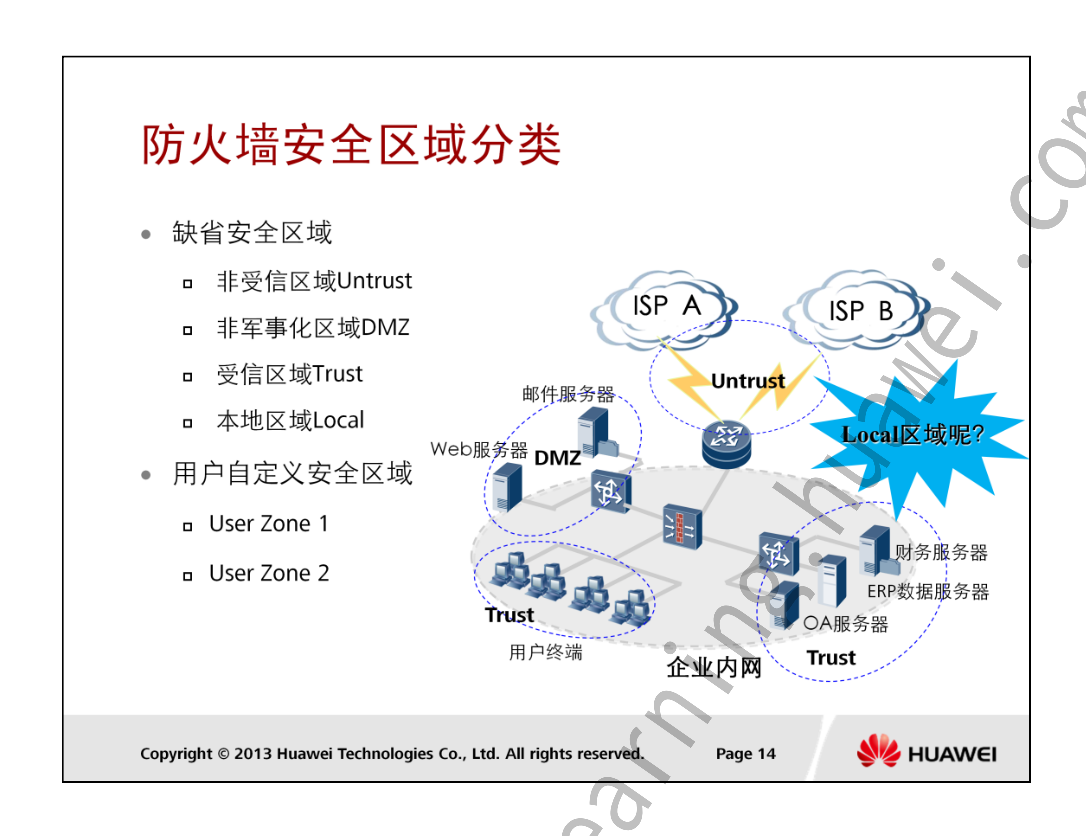


在此组网方式时，防火墙位于内部网络和外部网络之间时，与内部网络、外部网络相连的上下行业务接口均工作在三层，需要分别配置成不同网段的IP地址，防火墙负责在内部网络、外部网络中进行路由寻址，相当于路由器。

此组网方式，防火墙可支持更多的安全特性，比如NAT 、UTM等功能，但需要修改原网络拓扑，例如，内部网络用户需要更改网关，或路由器需要更改路由配置等。因此，做为设计人员需综合考虑网络改造、业务中断等因素。



- Zone的作用
  - 安全策略都基于安全区域实施
  - 在同一安全区域内部发生的数据流动是不存在安全风险的，不需要实施任何安全策略。
  - 只有当不同安全区域之间发生数据流动时，才会触发设备的安全检查，并实施相应的安全策略。
  - 在防火墙中，同一个接口所连网络的所有网络设备一定位于同一安全区域中，而一个安全区域可以包含多个接口所连的网络。



防火墙支持多个安全区域，缺省支持非受信区域（Untrust）、非军事化区域（DMZ）、受信区域（Trust）、本地区域（Local）四种预定义的安全区域外，还支持用户自定义安全区域。

防火墙缺省保留的四个安全区域相关说明如下：

- 非受信区域Untrust：低安全级别的安全区域，安全级别为5。
- 非军事化区域DMZ：中等安全级别的安全区域，安全级别为50。
- 受信区域Trust：较高安全级别的安全区域，安全级别为85。
- 本地区域Local：最高安全级别的安全区域，安全级别为100。

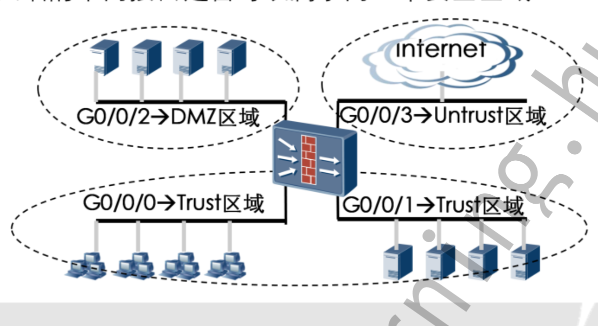
这四个安全区域无需创建，也不能删除，同时各安全级别也不能重新设置。安全级别用1 ～ 100 的数字表示，数字越大表示安全级别越高。

需要注意的是，将接口加入安全区域这个操作，实际上意味着将该接口所连网络加入到安全区域中，而该接口本身仍然属于系统预留用来代表设备本身的Local安全区域 。

USG防火墙最多支持32个安全区域。

防火墙安全区域与接口关系

- 安全区域与接口关系
  - 防火墙是否存在两个具有完全相同安全级别的安全区域?
  - 防火墙是否允许同一物理接口分属于两个不同的安全区域?
  - 防火墙的不同接口是否可以属于同一个安全区域?

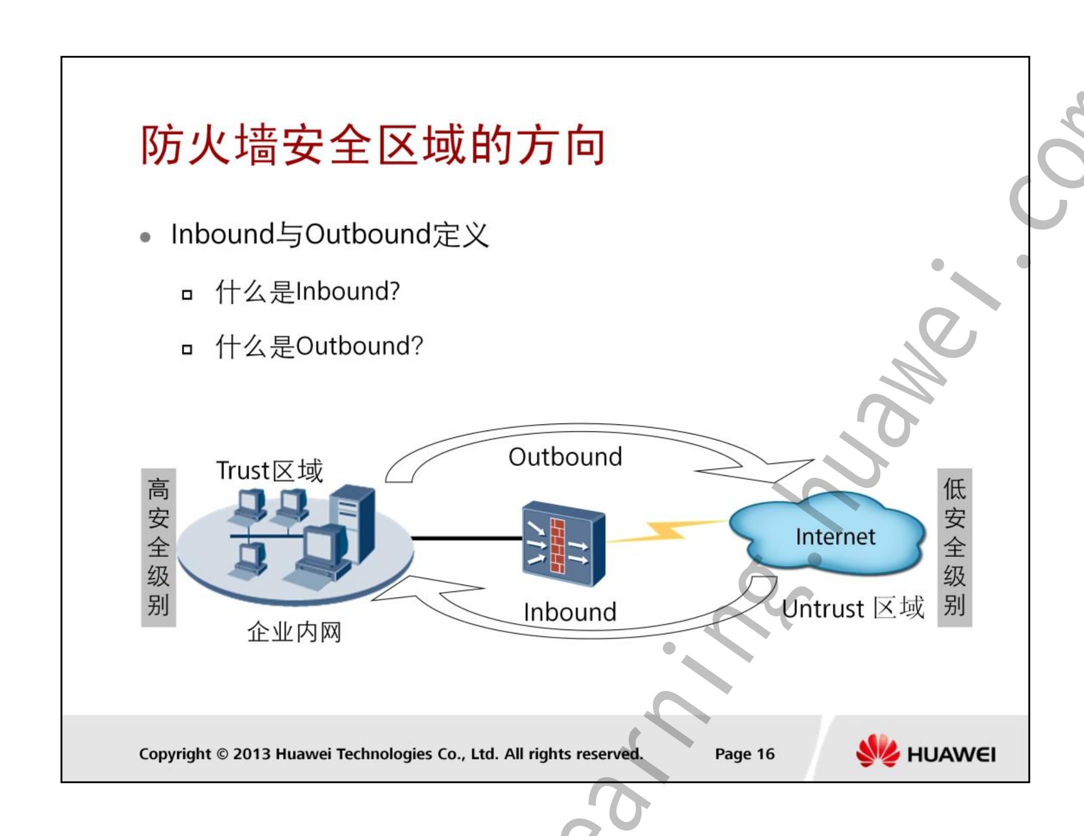


 Page 15 

在防火墙中是以接口为单位来进行分类，即同一个接口所连网络的所有网络设备一定位于同一安全区域中，而一个安全区域可以包含多个接口所连的网络。这里的接口既可以是物理接口，也可以是逻辑接口。所以可以通过子接口或者VLAN IF等逻辑接口实现将同一物理接口所连的不同网段的用户划入不同安全区域的功能。

思考:

1）若不同接口均属于同一个安全区域的场景下，域间安全转发策略是否会生效?



两个安全区域之间（简称安全域间）的数据流分两个方向:

- 入方向（inbound）：

  数据由低安全级别的安全区域向高安全级别的安全区域传输的方向；

- 出方向（outbound）：

  数据由高安全级别的安全区域向低安全级别的安全区域传输的方向；

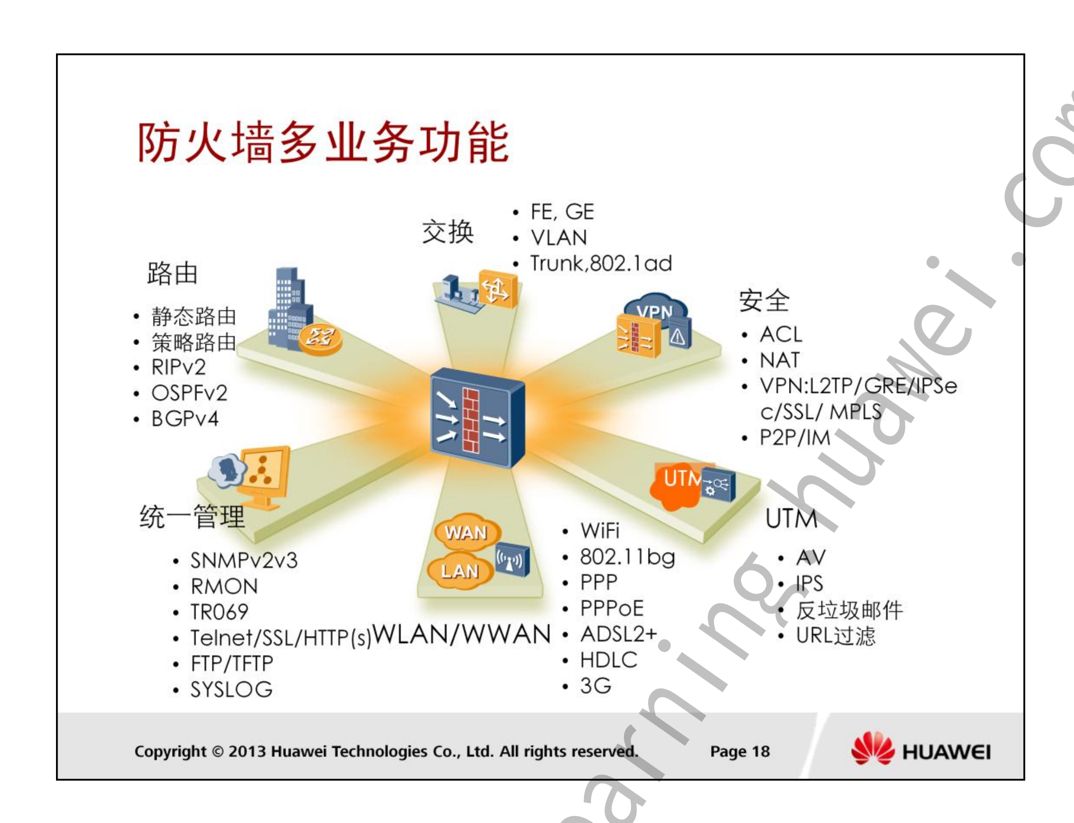
  高优先级与低优先级是相对的。

不同安全级别的安全区域间的数据流动都将激发USG防火墙进行安全策略的检查。可以事先为同一安全域间的不同方向设置不同的安全策略，当有数据流在此安全域间的两个不同方向上流动时，将触发不同的安全策略检查。



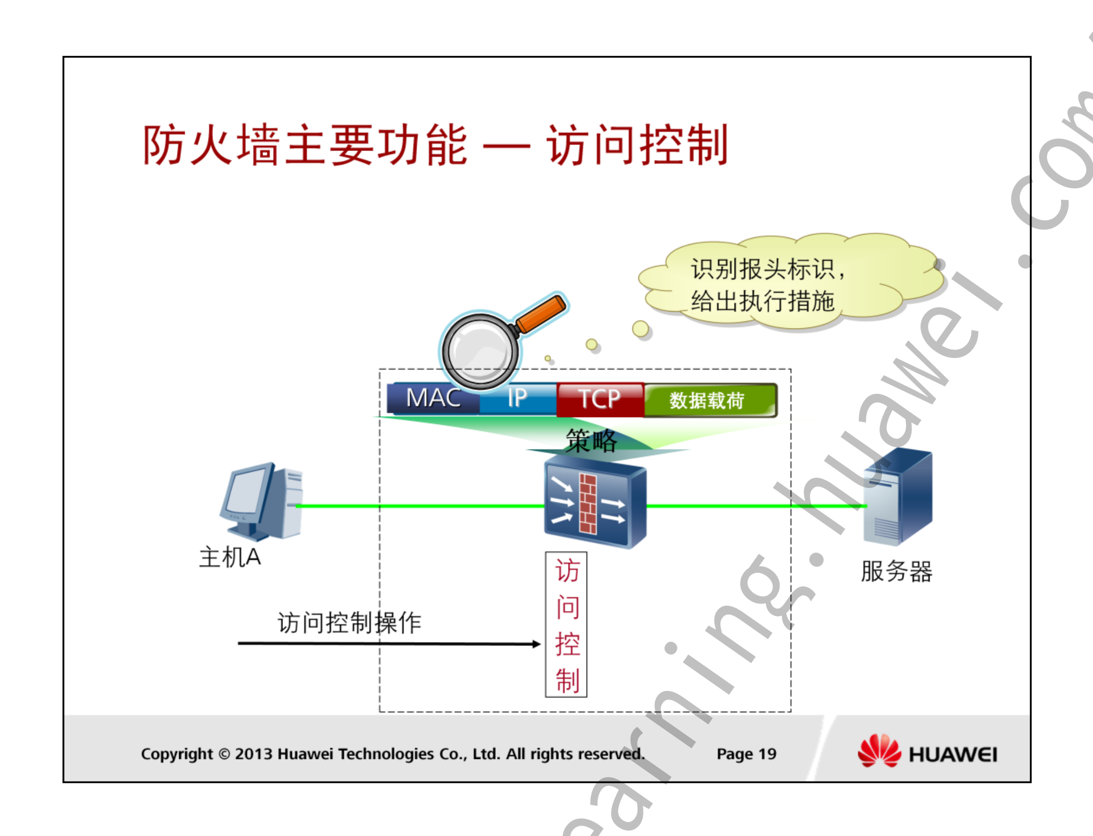
目录





防火墙支持以下特性：

- 路由
  - IPv4路由和IPv6路由
  - 支持静态路由
  - 支持RIP、OSPF、BGP、ISIS等动态路由
  - 支持路由策略和路由叠代
- 统一管理
  - SNMP
  - Web管理
  - NTP
- Ethernet
  - 支持二层、三层以太网接口。支持二层、三层以太网接口之间互相切换
  - Eth-Trunk和VLAN
- 安全
- UTM（统一威胁管理）
- 接入技术



防火墙的主要功能是策略（policy）和机制（mechanism）的集合，它通过对流经数据流的报文头标识进行识别，以允许合法数据流对特定资源的授权访问，从而防止那些无权访问资源的用户的恶意访问或偶然访问。

实现访问控制的主要工作过程如下：

1. 对于需要转发的报文，防火墙先获取报文头信息，包括IP 层所承载的上层协议的协议号、报文的源地址、目的地址、源端口号和目的端口号
2. 将报文头信息和设定的访问控制规则进行比较。
3. 根据比较结果，按照访问控制规则设定的动作，允许或拒绝对报文的转发。

防火墙基本功能—深度检测技术

- 基于特征字的识别技术
- 基于应用层网关识别技术
- 基于行为模式识别技术



 Page 20



深度报文检测（DPI，Deep packet inspection）是相对普通报文分析而言的一种新技术，普通报文检测仅仅分析IP包的四层以下的内容，包括源地址、目的地址、源端口、目的端口以及协议类型，而DPI则在此基础上，增加了对应用层的分析，可识别出各种应用及其内容。

针对不同的协议类型，识别技术一般可划分为以下三类。

- 基于特征字的识别技术

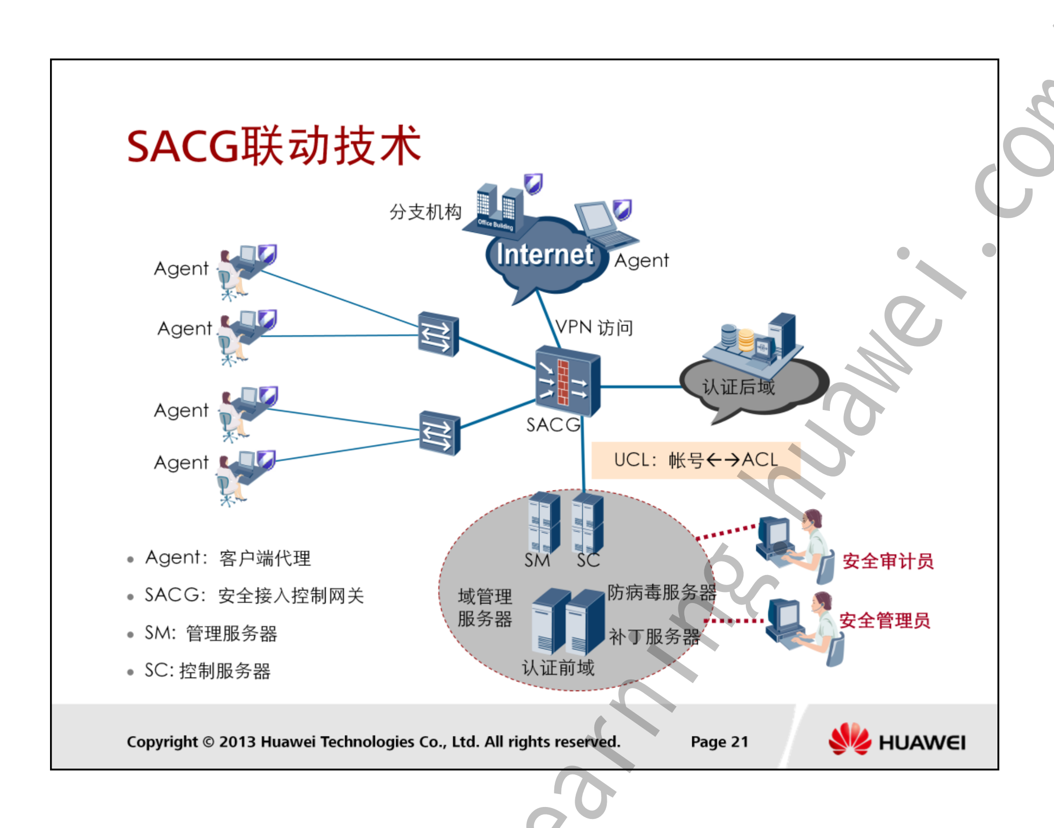
不同的应用通常会采用不同的协议，而各种协议都有其特殊的指纹，这些指纹可能是特定的端口、特定的字符串或者特定的Bit序列。基于特征字的识别技术，正是通过识别数据报文中的指纹信息来确定业务流所承载的应用。

- 基于应用层网关识别技术

我们知道，有一类业务的控制流与业务流是分离的，其业务流没有任何特征。例如，SIP、H323协议都属于这种类型的协议。SIP、H323通过信令交互过程，协商得到其数据通道，一般是RTP格式封装的语音流。也就是说，纯粹检测RTP流并不能确定这条RTP流是通过哪种协议建立起来的，只有通过检测SIP或H323的协议交互，才能得到其完整的分析。

- 基于行为模式识别技术

在实施行为模式识别技术之前，必须首先对终端的各种行为进行研究，并在此基础上建立起行为识别模型。从E-mail的内容看，垃圾邮件（SPAM）业务流发送邮件的速率、目的邮件地址数目、变化频率等参数，建立起行为识别模型，并以此分拣出垃圾邮件。



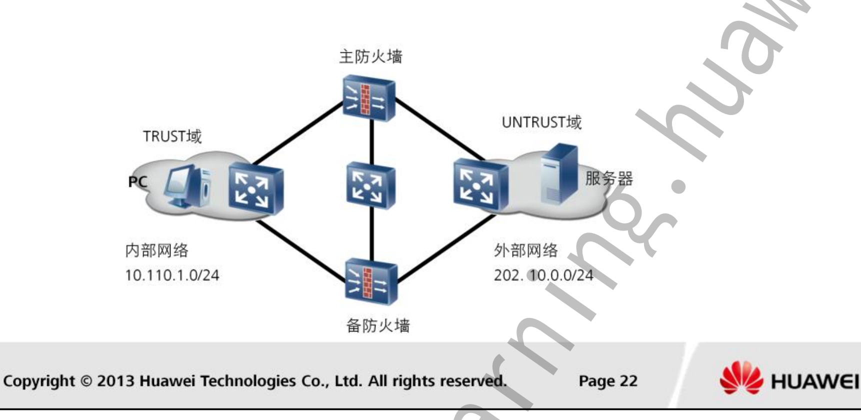
安全接入控制网关（Security Access Control Gateway，简称SACG）：控制终端的网络访问权限，对不同的用户，不同安全状况的用户开放不同的权限。由SC控制服务器对终端进行认证，并把结果通知SACG，SACG根据UCL策略决定终端的访问权限，防止外部用户访问企业内部网络，防止内部合法但不安全用户连接到企业网络进一步感染公司网络。

以SACG接入设备为参考点，内部网络划分为主要的三个逻辑区域：

接入区域：接入区域由一组客户端组成，这些客户端安装了TSM代理Agent，通过二层交换或者三层交换组成一个本地网络；

认证前域：认证前域是一个逻辑区域，通过对SACG进行ACL配置，可以确保用户在获得接入授权之前，只能访问ACL指定的网络或者主机。终端安全管理系统的认证前域主要包括SM管理服务器、SC控制服务器、AD域管理服务器、防病毒服务器、补丁服务器等；

认证后域：认证后域是一个逻辑区域，与认证前域相对应。通过对SACG进行配置，当用户获得业务授权后，就可以访问认证后域的业务资源。比如OA业务服务器、ERP业务服务器、财务服务器等；



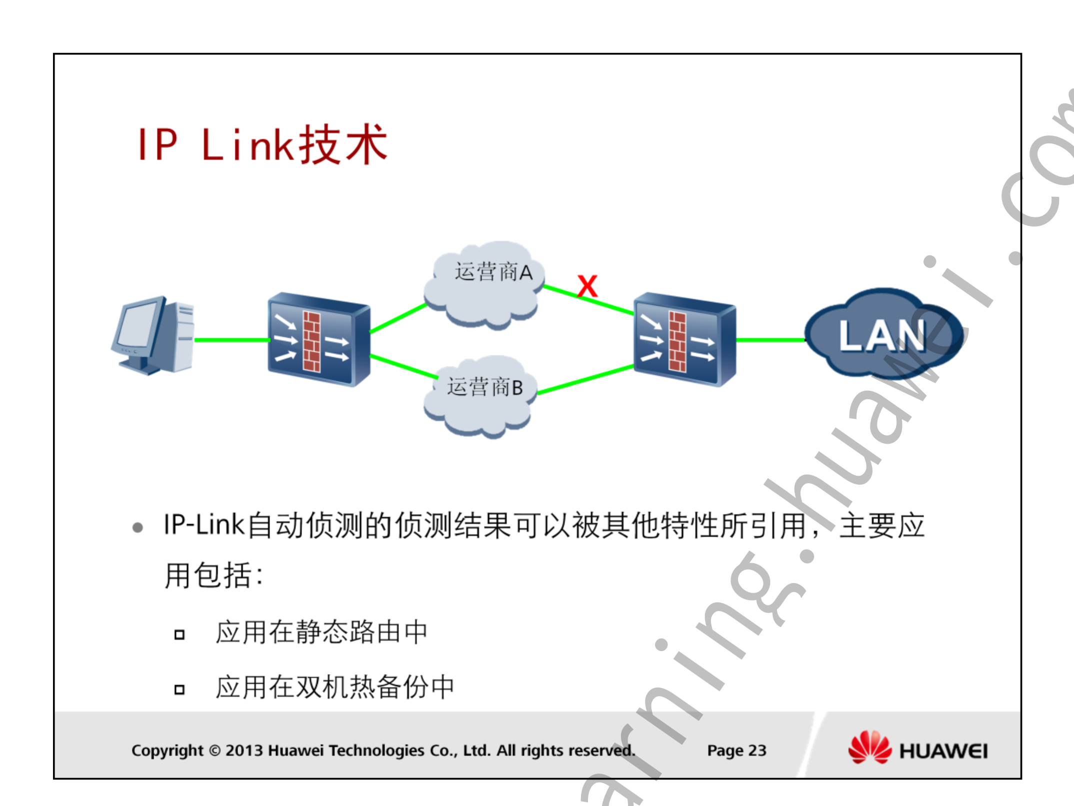
通常，内部网络的主机都配置一条缺省路由，下一跳为出口路由器的接口IP地址。内外部用户的交互报文全部通过Router。如果Router出现故障，内部网络中所有以Router为缺省路由下一跳的主机与外部网络之间的通讯将中断，通讯可靠性无法保证。

虚拟路由冗余协议（VRRP, Virtual Router Redundancy Protocol）将局域网的一组路由器组织成一个虚拟路由器，称之为一个备份组。其中，仅有一台设备处于活动状态，称为主用设备（Master）；其余设备都处于备份状态。

借助VGMP机制，可以实现对多个VRRP备份组的状态一致性管理、抢占管理和通道管理等，保证一台防火墙上的接口同时处于主用或备用状态，实现防火墙防火墙VRRP状态的一致性。

另外，启动HRP功能后，Master和Backup设备之间将实时同步关键配置命令和会话表状态信息。如果Master设备发生故障，导致VRRP管理组状态改变，引起VRRP备份组抢占，从而实现Backup设备平滑地接替工作。

详细内容将在后面章节进行详细介绍。



- 链路可达检测功能

IP-Link自动侦测是利用ICMP或者ARP协议的特征对业务链路正常与否进行的自动侦测。它定时地向指定的目的IP地址发送ICMP或者ARP请求，等待相应目的IP地址的回应，根据回应的情况判断网络的连通状况。

如果在设定的时限内未收到回应报文，则认为链路发生故障，并进行后续相应的操作。当原来认为发生故障的链路，在之后设定的时限内，有连续3个回应报文返回，则认为发生故障的链路已经恢复正常，此后进行链路恢复的相关操作。

IP-Link自动侦测的侦测结果（目的主机可达或者不可达）可以被其他特性所引用，主要应用包括：

- 应用在静态路由中

当IP-Link侦测出链路不可达时，防火墙会对自身的静态路由进行相应的调整。如原来高优先级的静态路由所经链路被检测到发生故障，防火墙会选择新的链路进行业务转发。如果高优先级的静态路由链路故障恢复正常时，防火墙又会进行静态路由的调整，用高优先级的路由替换低优先级的路由，保证每次用到的链路是最高优先级的并且是可达的，以保持业务的持续进行。

- 应用在双机热备份中

当IP-Link侦测出链路不可达时，防火墙会对自身VGMP的优先级进行相关调整，引发主备切换，从而保证业务能够持续流通。

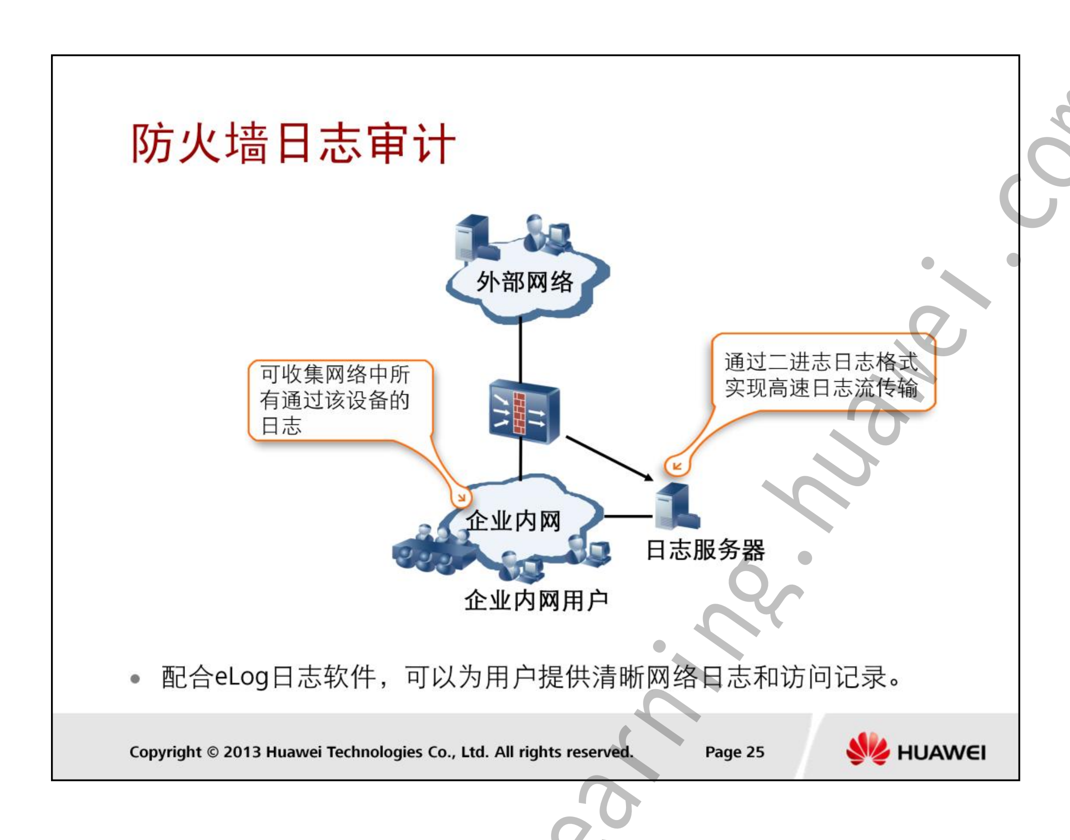


QoS提供的主要的流量管理技术包括：流分类、流量监管、流量整形、拥塞管理和拥塞避免是实现有区别地实施服务的基础。它们主要完成如下功能：

- 流分类依据一定的匹配规则识别出对象，是有区别地实施服务的前提。
- 流量监管对进入网络的特定流量的规格进行监管。当流量超出规格时，可以采取限制或惩罚措施，以保护客户的商业利益和网络资源不受损害。
- 流量整形限制从某一网络流出的某一连接的流量，使这一流量的报文以比较均匀的速度向外发送，是一种主动调整流量输出速率的措施。
- 拥塞管理是一种当拥塞发生时制定资源的调度策略从而决定报文转发时的处理次序的机制，主要调度策略包括FIFO、CQ、PQ、WFQ、RTP等队列。

说明： 对于三层接口，USG5500只有在接口上配置了接口限速功能后，接口上的队列功能才会生效，基于类的WRR功能不受该限制。

- 拥塞避免是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞有加剧的趋势时，主动丢弃报文，通过调整网络的流量来解除网络过载的一种流控机制。



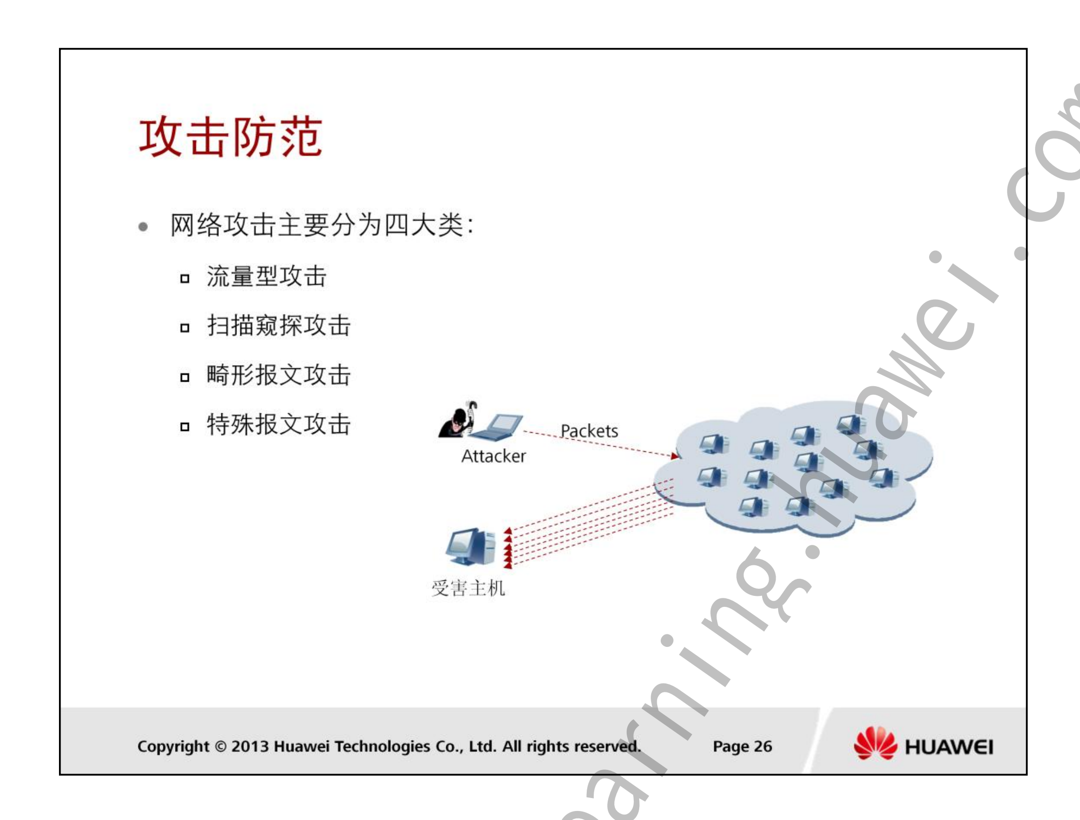
Elog是华为防火墙专用的日志软件，可以支持通用的Syslog日志和二进制日志。

- Syslog日志

像普通系统日志以及流量监控日志（除DPI流量监控日志外）采用Syslog方式以文本格式进行输出。这些日志信息必须通过信息中心模块进行日志管理和输出重定向，然后显示在终端屏幕上，或者发送给日志主机进行存储和分析。

- 二进制日志

像会话日志中NAT/ASPF产生的日志、DPI流量监控日志，对于这种类型的日志提供了一种“二进制”输出方式，直接输出到二进制日志主机以便对日志进行存储和分析，无需信息中心模块的参与。



- 流量型攻击

流量型攻击是指攻击者通过大量的无用数据占用过多的资源以达到服务器拒绝服务的目的。

- 扫描窥探攻击

扫描窥探攻击主要包括IP地址扫描和端口扫描，从而准确的发现潜在的攻击目标。

- 畸形报文攻击

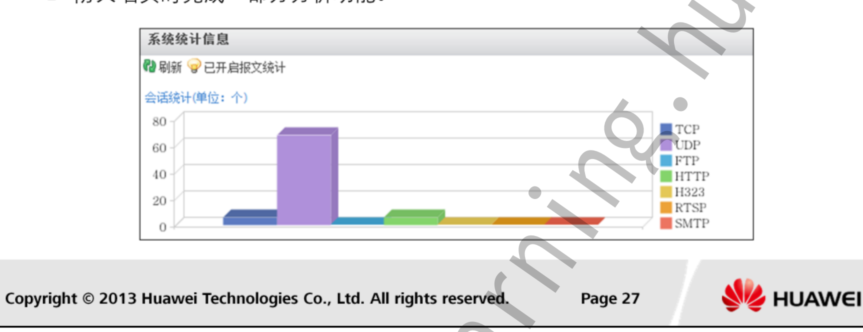
畸形报文攻击是指通过向目标系统发送有缺陷的IP报文。主要的畸形报文攻击有Ping of Death、Teardrop等。

- 特殊报文攻击

特殊报文攻击是指攻击者利用一些合法的报文对网络进行侦察或者数据检测，这些报文都是合法的应用类型，只是正常网络很少用到。

防火墙报文统计

- 报文统计
  - 对于防火墙来说，不仅要对数据流量进行监控，还要对内外部网络之间的连接发起情况进行检测，因此要进行大量的统计、计算与分析。
- 防火墙对报文统计结果的分析有如下两个方面：
  - 专门的分析软件事后分析日志信息。
  - 防火墙实时完成一部分分析功能。

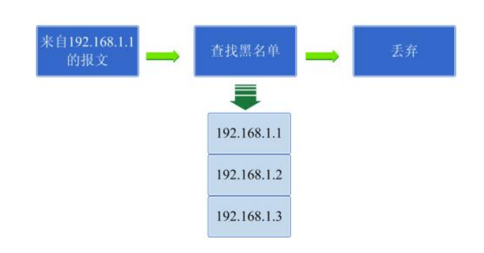


 Page 27 HUAWEI

通过对报文统计分析，防火墙实现了对内部网络的保护。如：

- 通过分析外部网络向内部网络发起的TCP 或UDP 连接总数是否超过设定的阈值，可以确定是否需要限制该方向的新连接发起，或者限制向内部网络某一IP地址发起新连接。
- 通过分析发现系统的总连接数超过阈值，则可以加快系统的连接老化速度，以保证新连接能够正常建立，防止因系统太忙而导致拒绝服务情况的发生。

防火墙黑名单



- 黑名单
  - 黑名单是一个IP地址列表。防火墙将检查报文源地址，如果命中，丢弃所有报文
  - 快速有效地屏蔽特定IP地址的用户。
- 创建黑名单表项，有如下两种方式：
  - 通过命令行手工创建。
  - 通过防火墙攻击防范模块或IDS模块动态创建。

 Page 28



防火墙动态创建黑名单的工作过程如下：

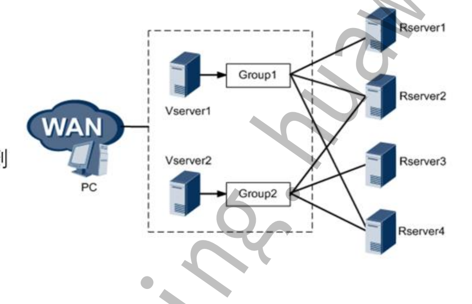
1. 根据报文的行为特征检测到来自特定IP地址的攻击企图。
2. 自动将这一特定IP地址插入黑名单表项。
3. 防火墙根据黑名单丢弃从该IP地址发送的报文，从而保障网络安全。

通过在黑名单中引用高级ACL，可绑定黑名单和高级ACL，确保一些特殊用户免受黑名单的干扰。此时的安全策略是根据高级ACL规则确定是否允许该报文通过。对于ACL规则拒绝的流量进行丢弃，而ACL规则允许的流量则允许通过，此时即使用户被加入黑名单，仍能正常通信。

负载均衡

- 负载均衡。
  - 将访问同一个IP地址的用户流量分配到不同的服务器上。
- 负载均衡采用以下技术，将用户流量分配到多台服务器：
  - 虚服务技术
  - 服务器健康性检测
  - 基于流的转发

    即通过指定算法，将数据流发送到各个真实服务器进行处理。



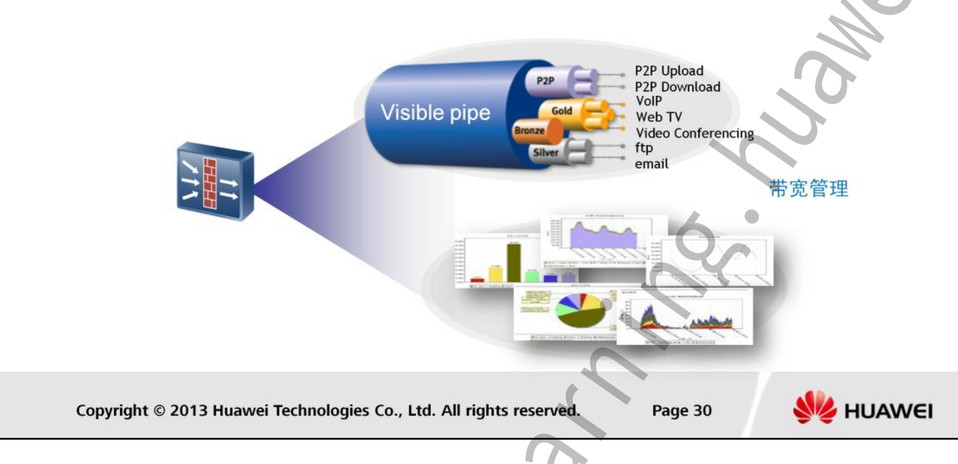
 Page 29 

负载均衡采用以下技术，将用户流量分配到多台服务器：

- 虚服务技术。防火墙配置负载均衡功能后，多个服务器共用一个公网IP地址（即虚拟IP地址），这些服务器被称作真实服务器。用户对这些真实服务器上内容的访问都通过该虚拟IP地址进行。每一个真实服务器使用不同的私网IP地址（即实IP地址），由多层交换机/防火墙将访问虚拟IP地址的流量按照预先配置的算法分配到每一个真实服务器。
- 服务器健康性检测。即防火墙通过周期性的探测真实服务器，实现健康性检查功能。真实服务器如果可用，则返回应答报文；如果不可用，一段时间后防火墙将禁止该真实服务器，将流量按配置好的策略分配到其他的实服务器上。
- 基于流的转发。即通过指定算法，将数据流发送到各个真实服务器进行处理。

应用控制

- DPI（Deep Packet Inspection），即深度报文检测技术。使用DPI知识库中的规则，对P2P、VoIP、Video等多种应用数据，可以对识别的网络流量进行允许通过、阻断、限制连接数和限速等控制动作。



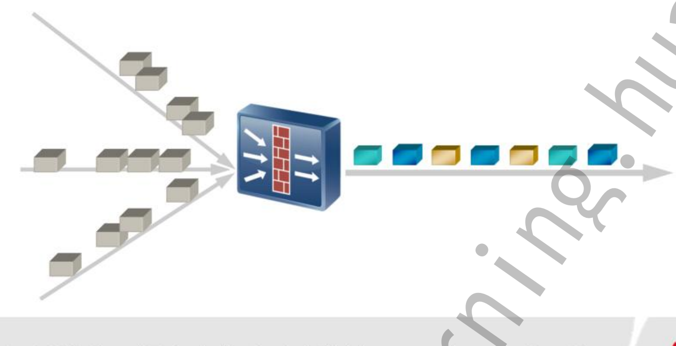
 Page 30 HUAWEI

DPI（Deep Packet Inspection），即深度报文检测技术，是对数据流中的应用层数据进行内容检测的技术。对通过解析的数据包，使用DPI知识库中的规则，对应用数据进行匹配，分析报文或流在IP和UDP/TCP层以上的应用类型。

在匹配成功后，根据应用的需求，可以对识别的网络流量进行允许通过、阻断、限制连接数和限速等控制动作。

防火墙性能指标 — 吞吐量

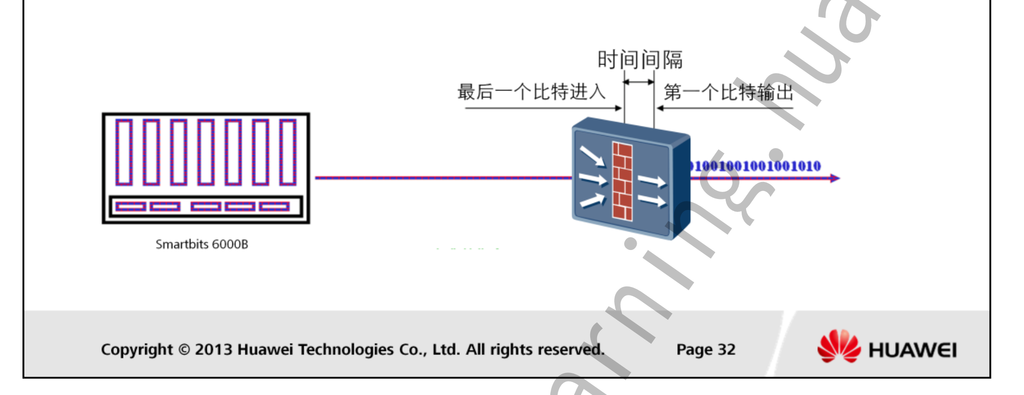
- 吞吐量：防火墙能同时处理的最大数据量
- 有效吞吐量：除掉TCP因为丢包和超时重发的数据，实际的每秒传输有效速率



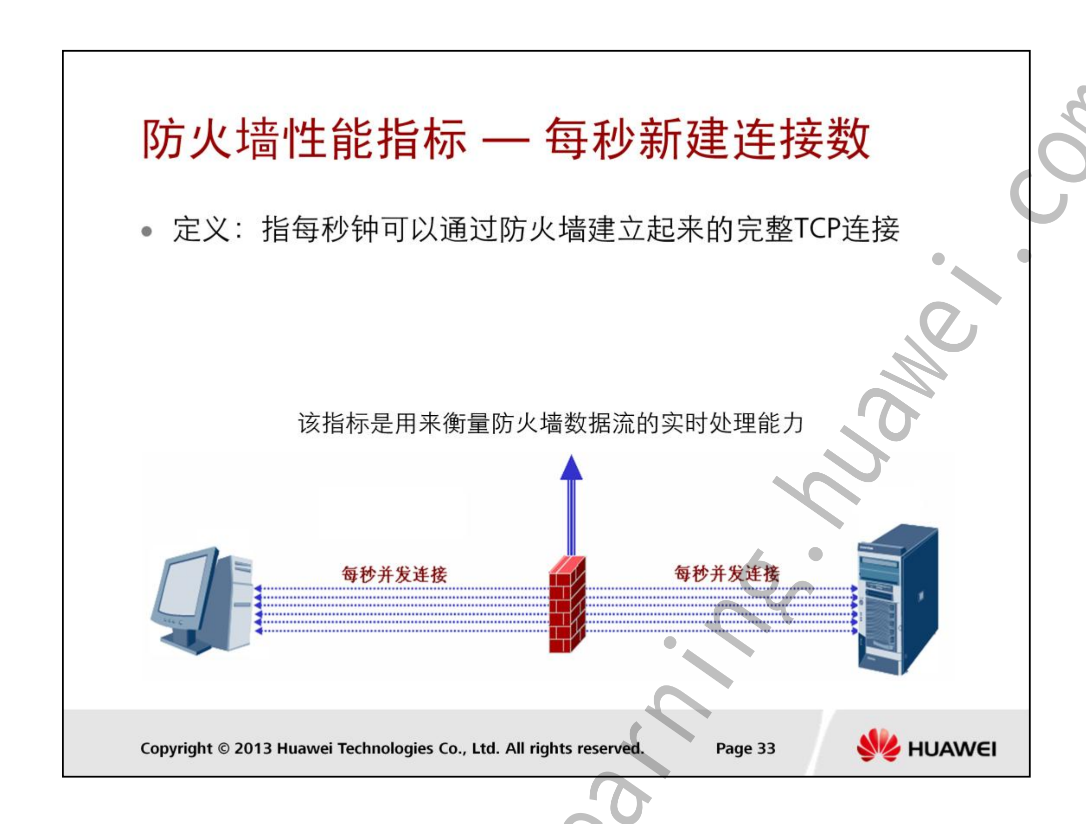
 Page 31



吞吐量是指防火墙对报文的处理能力。RFC2647中定义，防火墙的吞吐量是指防火墙对指定的数据载荷每秒钟接收、处理并正确转发到目的接口的比特数。在测试防火墙吞吐量时将忽略错误流量以及重传的流量，即只计算能够正确转发到目的接口的流量；另外防火墙吞吐量还需要对不同载荷级别的流量、不同方向的流量等进行测试，最终取平均值。对于载荷级别，业界一般都是使用1K～1.5Kbyte的大包来衡量防火墙对报文的处理能力。但网络流量大部分是200Byte的报文，因此测试时还应考虑小包吞吐量。同时由于防火墙需要配置规则，因此还需要测试防火墙支持ACL下的转发性能。



数据包的最后一个比特进入防火墙到第一个比特输出防火墙的时间间隔指标，是用于测量防火墙处理数据的速度理想的情况。



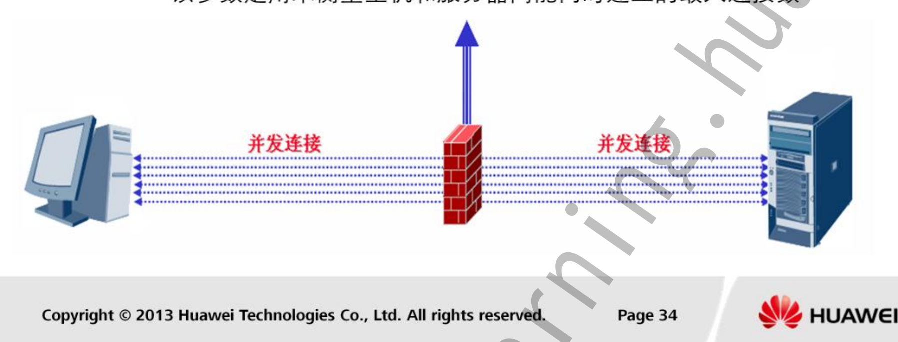
每秒新建连接数指的是每秒钟可以通过防火墙建立起来的完整TCP连接。

由于防火墙的连接是根据当前通信双方状态而动态建立的。每个会话在数据交换之前，在防火墙上都必须建立连接。如果防火墙建立连接速率较慢，在客户端反映是每次通信有较大延迟。因此支持的指标越大，转发速率越高。在受到攻击时，这个指标越大，抗攻击能力越强；另外这个指标越大，状态备份能力也越强。

防火墙性能指标 — 并发连接数

- 定义：由于防火墙是针对连接进行处理报文的，并发连接数目是指的防火墙可以同时容纳的最大的连接数目，一个连接就是一个TCP/UDP的访问。

该参数是用来衡量主机和服务器间能同时建立的最大连接数



并发连接数指的可以同时容纳的最大的连接数目。

由于防火墙是针对连接进行处理报文的，并发连接数目是指的防火墙可以同时容纳的最大的连接数目，一个连接就是一个TCP/UDP的访问。并发连接数指标越大，抗攻击能力也越强。当防火墙上并发连接数达到峰值后，新的连接请求报文到达防火墙时将被丢弃。



目录



防火墙设备管理概述

- 设备登录管理
  - Console登录
  - Web登录
  - telnet登录
  - SSH登录
- 设备文件管理
  - 配置文件管理
  - 系统文件管理（软件升级）
  - License管理



 Page 36



- 设备登录管理

Console:通过RS-232配置线连接到设备上，使用Console方式登录到设备上，进行配置。

Telnet:　通过PC终端连接到网络上，使用Telnet方式登录到设备上，进行配置。

Web：　在客户端通过Web浏览器访问设备，进行控制和管理。

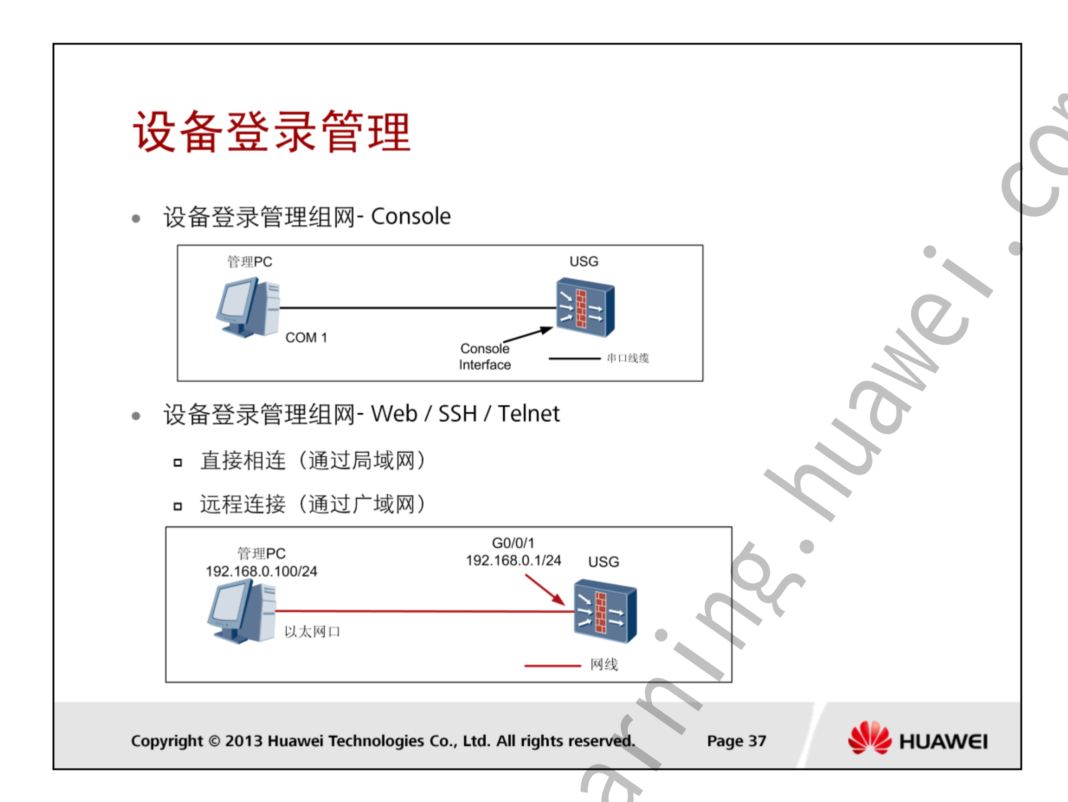
SSH:　提供安全的信息保障和强大认证功能，保护设备系统不受IP欺骗、明文密码截取等攻击。

- 设备文件管理

配置文件是设备启动时要加载的配置项。用户可以对配置文件进行保存、更改和清除、选择设备启动时加载的配置文件等操作。系统文件包括USG设备的软件版本，特征库文件等。一般软件升级需要管理系统文件。

系统软件升级。上传系统软件到设备可通过TFTP方式和FTP方式上传系统软件到设备上。升级系统软件 配置设备下次启动时使用的软件系统。

License是设备供应商对产品特性的使用范围、期限等进行授权的一种合约形式，License可以动态控制产品的某些特性是否可用。



- 通过Console口登录：

使用PC终端通过连接设备的Console口来登录设备，进行第一次上电和配置。当用户无法进行远程访问设备时，可通过Console进行本地登录；当设备系统无法启动时，可通过console口进行诊断或进入BootRom进行系统升级。

- 通过Telnet登录：

通过PC终端连接到网络上，使用Telnet方式登录到设备上，进行本地或远程的配置，目标设备根据配置的登录参数对用户进行验证。Telnet登录方式方便对设备进行远程管理和维护。

- 通过SSH登录：

提供安全的信息保障和强大认证功能，保护设备系统不受IP欺骗、明文密码截取等攻击。SSH登录能更大限度的保证数据信息交换的安全。

- 通过Web登录：

在客户端通过Web浏览器访问设备，进行控制和管理。适用于配置终端PC通过Web方式登录。

注意：PC和USG以太网口的IP地址必须在同一网段或PC和USG之间有可达路由。

通过Console口登录设备

- USG配置口登录的缺省用户名为admin，缺省用户密码为Admin@123。其中，用户名不区分大小写，密码要区分大小写。





 Page 38



如果使用PC进行配置，需要在PC上运行终端仿真程序（如Windows3.1的Terminal，Windows98/Windows2000/Windows XP的超级终端），建立新的连接。如图所示，键入新连接的名称，单击“确定”。

在串口的属性对话框中设置波特率为9600，数据位为8，奇偶校验为无，停止位为1，流量控制为无，单击“确定”，返回超级终端窗口。

打开设备电源开关。设备上电后，检查设备前面板上的指示灯显示是否正常。

通过Web方式登录设备

- 设备缺省可以通过GigabitEthernet0/0/0接口来登录Web界面。
  - 将管理员PC的网络连接的IP地址获取方式设置为“自动获取IP地址”。
  - 将PC的以太网口与设备的缺省管理接口直接相连，或者通过交换机中转相连。
  - 在PC的浏览器中访问http://192.168.0.1，进入Web界面的登录页面。
  - 缺省用户名为admin，密码为Admin@123





缺省情况下，设备开启HTTP；建议开启HTTPS，提高安全性。用户可以通过用户名/密码：admin/Admin@123登录，为保证系统安全，登录后请修改密码。

只有GigabitEthernet 0/0/0接口加入Trust域并提供缺省IP地址（192.168.0.1/24），并开放Trust域到Local域的缺省包过滤，方便初始登录设备。

缺省情况下开放Local域到其他任意安全区域的缺省包过滤，方便设备自身的对外访问。

其他接口都没有加安全区域，并且其他域间的缺省包过滤关闭。要想设备转发流量必须将接口加入安全区域，并配置域间安全策略或开放缺省包过滤。

Web登录配置管理

- 配置USG的IP地址。(略)
- 配置USG接口Web设备管理。

  [USG-GigabitEthernet0/0/1] service-manage enable

  [USG-GigabitEthernet0/0/1] service-manage http permit
- 启动Web管理功能。

  [USG] web-manager security enable port 2000
- 配置Web用户。

  [USG] aaa

  [USG-aaa] local-user webuser password cipher Admin@123

  [USG-aaa] local-user webuser service-type web

  [USG-aaa] local-user webuser level 3

 Page 40



- 开启HTTP

  执行命令system-view，进入系统视图。

  执行命令web-manager enable [port port-number]，开启HTTP。

  此时在Web浏览器中应该通过http://格式的地址登录设备。默认端口号是80。
- 开启HTTPS（默认证书）

  执行命令system-view，进入系统视图。

  执行命令web-manager security enable port port-number，开启HTTPS。

  此时在Web浏览器中应该通过https://格式的地址登录设备。
- local-user level命令用来配置本地用户的优先级。

  Level 3：管理级



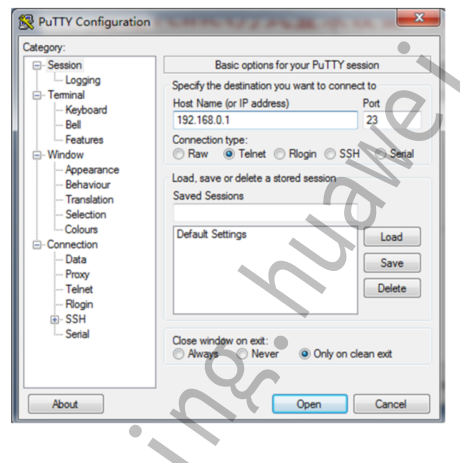
启动Web管理功能，根据客户需求启动HTTP或者HTTPS管理，以及设置端口号。

开启HTTP/HTTPS服务后（设备作为Web服务器），配置终端通过HTTP/HTTPS协议（Web方式）登录设备，实现远程配置和管理。相比HTTP，HTTPS具有更高的安全性。在一个需要更高安全保证的网络环境下，建议使用HTTPS服务。

1. 选择“系统 > 管理员 > 设置”。
2. 选中“HTTP服务”或“HTTPS服务”对应的“启用”。 可以同时开启HTTP服务和HTTPS服务。
3. 在“HTTP服务端口”或“HTTPS服务端口”中输入端口号。
4. 单击“应用”。

通过Telnet方式登录设备

- 设备缺省可以通过GigabitEthernet0/0/0接口来实现Telnet登录。
  - 将管理员PC的网络连接的IP地址获取方式设置为“自动获取IP地址”。
  - 通过Putty telnet192.168.0.1，进入登录页面。
  - 缺省用户名为admin，密码为Admin@123





GigabitEthernet 0/0/0接口加入Trust域并提供缺省IP地址（192.168.0.1/24），并开放Trust域到Local域的缺省包过滤，方便初始登录设备。

Telnet登录配置管理

- 配置USG接口telnet设备管理。

  [USG-GigabitEthernet0/0/1] service-manage enable

  [USG-GigabitEthernet0/0/1] service-manage telnet permit

- 配置vty interface。

  [USG] user-interface vty 0 4

  [USG-ui-vty0-4] authentication-mode aaa

  [USG-ui-vty0-4] protocol inbound telnet

- 配置Telnet用户信息。

  [USG] aaa

  [USG-aaa] local-user user1 password cipher password@123

  [USG-aaa] local-user user1 service-type telnet

  [USG-aaa] local-user user1 level 3

 Page 43 

USG提供两种验证方式来检查远端Telnet用户的合法性，分别是密码验证和AAA验证。

- 使用密码方式远程Telnet
  - 验证方式为密码验证时，远端用户登录到USG只需要输入密码。
  - 执行命令user-interface [interface-type] first-number [last-number]，进入VTY用户界面视图。
  - 执行authentication-mode password，配置验证方式为密码验证。
  - 执行set authentication password cipher password，设置Password验证的密码
- 使用AAA方式远程Telnet
  - 执行命令user-interface [interface-type] first-number [last-number]，进入VTY用户界面视图。
  - 执行命令authentication-mode aaa，配置验证方式为AAA验证。
  - 执行命令protocol inbound { all | telnet }，配置用户界面支持Telnet协议。
  - 执行命令aaa，进入AAA视图。
  - 执行命令local-user user-name password cipher password，创建本地用户。
  - 执行命令local-user user-name service-type telnet，配置本地用户的服务类型为telnet。
  - 执行命令local-user user-name level level，配置本地用户的级别。


Telnet登录配置管理
配置Telnet管理员
系统
管理员
管理员
管理员密码管理配置
密码管理
启用
密码过期时间
90
<30-365>（天）
应用
管理员列表
新建
删除
刷新
按用户名查询
请输入用户名
查询
用户名
用户级别
新建管理员和管理员级别。
Note：不需要设置Web，FTP，Telnet等类别。默认支持所有用户类别。
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 44
HUAWEI

通过SSH方式登录设备 (1)

- 配置USG的接口IP地址。（略）
- 配置USG接口telnet设备管理。

```
[USG-GigabitEthernet0/0/1] service-manage enable
[USG-GigabitEthernet0/0/1] service-manage telnet permit
```

- 配置RSA本地密钥对。

```
<USG> system-view
[USG] rsa local-key-pair create
It will take a few minutes. Input the bits in the modulus[default = 512]:512
Generating keys... ..++++++++++++ ..............................
```

- 配置VTY用户界面。

```
[USG] user-interface vty 0 4
[USG-ui-vty0-4] authentication-mode aaa
[USG-ui-vty0-4] protocol inbound ssh
```

 Page 45 

SSH可以为用户登录设备系统提供安全的信息保障和强大的认证功能。配置USG接口SSH设备管理，管理员根据实际的需要打开。

在USG上生成本地密钥对。

成功完成SSH登录的首要操作是：配置并产生本地RSA密钥对。请您在进行其它SSH配置之前，一定记得完成**rsa local-key-pair create**配置，生成本地密钥对。此命令只需执行一遍，设备重启后不必再次执行。

通过SSH方式登录设备 (2)

- 新建用户名为Client001的SSH用户，且认证方式为password。

  [USG] ssh user client001

  [USG] ssh user client001 authentication-type password

- 为SSH用户Client001配置密码为Admin@123。

  [USG] aaa

  [USG-aaa] local-user client001 password cipher Admin@123

  [USG-aaa] local-user client001 service-type ssh

- 配置SSH用户Client001的服务方式为STelnet，并启用STelnet服务。

  [USG] ssh user client001 service-type stelnet

  [USG] stelnet server enable

以上配置完成后，运行支持SSH的客户端软件，建立SSH连接。

 Page 46



- 在USG上创建SSH用户。

  设备作为SSH服务器时，可配置对SSH用户的验证方式为Password、RSA方式。

  上图以Password为例。

- 启用USG的服务方式为STelnet/SFTP服务。
  - 执行命令ssh user user-name service-type { sftp | stelnet | all }，为SSH用户配置服务方式。
  - 在使用SSH1.5版本配置SSH终端服务时，不需进行该配置；在使用SSH2.0版本配置SSH终端服务时，必须配置该命令。
- 启用USG的STelnet/SFTP服务。
  - 配置SSH服务器功能。

▪ 执行命令stelnet server enable，启用Stelnet服务。

▪ 在使用SSH1.5版本配置SSH终端服务时，不需进行该配置；在使用SSH2.0版本配置SSH终端服务时，必须配置该命令。

配置文件管理

- 配置文件类型
  - saved-configuration
  - current-configuration
- 配置文件操作
  - 保存配置文件
  - 擦除配置文件（恢复出厂配置）
  - 配置下次启动时的系统软件和配置文件
  - 重启设备

 Page 47 

- saved-configuration:
  - USG设备下次上电启动时所用的配置文件，存储在USG的Flash或者CF卡，重启不会丢失。
- current-configuration:
  - USG设备当前生效的配置，命令行和Web操作都是修改current-configuration。存储在USG的内存中，重启丢失。
- 保存配置
  - 作用：为了使当前配置能够作为防火墙下次上电时的起始配置。
  - 方法1 (命令行)：在用户视图下，执行命令save。
  - 方法2 (Web)：选择“主页”右上方的“保持”按钮。如下图所示。
- 重启防火墙
  - 作用：防火墙将重新启动，并将重启动作记录至日志中。
  - 方法1 命令行：在用户视图下，执行命令reboot命令。
  - 方法2 Web：选择“系统 >维护>系统重启”如图所示。

配置文件管理

- 配置文件类型
  - saved-configuration
  - current-configuration
- 配置文件操作
  - 保存配置文件
  - 擦除配置文件（恢复出厂配置）
  - 配置下次启动时的系统软件和配置文件
  - 重启设备

 Page 48 

- 擦除配置文件。
  - 作用：配置文件被擦除后，防火墙下次上电将采用缺省的配置参数进行初始化。

  方法1(命令)：在用户视图下，执行命令reset saved-configuration。

  方法2(Web)：选择“系统 >维护>配置管理”，执行恢复出厂配置按钮

  方法3（硬件reset按钮）：如果设备没有上电：先按住RESET按钮，再打开电源开关。当面板上设备指示灯同时以2次/秒的频率闪烁时，松开RESET按钮，设备会使用缺省配置启动。

  方法4（硬件reset按钮）：如果设备已经正常启动：长时间（超过10秒）按住RESET。设备将重启并使用缺省配置进行启动。
- 配置下次启动时的系统软件
  - 命令行：在用户视图下，执行命令startup system-software sysfile。
  - Web：选择“系统 >维护>系统更新”，“选择”下次启动系统软件按钮。

版本升级(命令行)

- 使用TFTP下载文件
  - 执行命令tftp tftp-server-address or hostname get source-filename [destination-filename]
- 使用FTP下载文件
  - 执行命令ftp ip-address [port-number] [vpn-instance vpn-instance-name]，与FTP服务器建立控制连接，并进入FTP客户端视图。

  注：以上两种下载文件的方式二选一即可
- 配置系统下次启动时使用的系统软件
  - 执行startup system-software sys-filename。

 Page 49 

- 通过TFTP方式
  - USG作为TFTP客户端从TFTP服务器上获得系统软件。这种情况下，不要求TFTP服务器和USG在同一个网段，只要保证二者之间路由可达即可。
- 通过FTP方式

  这种情况下，不要求FTP服务器和USG在同一个网段，只要保证二者之间路由可达即可。
  - USG作为FTP客户端。
    - 在FTP主机上运行FTP服务器程序，并把需要下载的系统软件放到相应的FTP的工作目录下，在USG用户视图下，通过命令下载系统软件到USG的相应目录下，具体操作请参见上传、下载文件。
  - USG作为FTP服务器。
    - 在USG上启动FTP服务器，通过FTP客户端登录到USG后，把系统软件上传到USG相应的目录下。



- 一键升级系统软件
    - 如果当前设备的存储空间不足，设备将自动删除当前运行的系统软件。
- 系统软件必须以“.bin”作为扩展名，不支持中文。
    - 选择“系统 > 维护 > 系统更新”。
    - 单击“一键式版本升级”，显示一键系统软件升级向导界面。
    - 可选：依次单击“导出”，将设备上的告警信息、日志信息和配置信息导出到终端。建议将配置信息保存到终端。
    - 单击“浏览”，选择待上传的系统软件。
    - 根据当前网络是否允许设备升级后立即重启，选中“设置为下次启动系统软件，并重启系统”或“设置为下次启动系统软件，不重启系统”前的单选框。
    - 重启设备后，才能使用升级后的系统软件。

License配置

- License是设备供应商对产品特性的使用范围、期限等进行授权的一种合约形式，License可以动态控制产品的某些特性是否可用。
- 激活License
  - 执行命令**system-view**，进入系统视图。
  - 执行命令**license file** *license-file*，激活指定的License文件。
  - 可以通过命令**display license**，查看License的信息。

点击此处，上传将要激活的License文件





- 手动激活License
  - License文件必须以“.dat”作为扩展名，不支持中文。
    - 选择“系统 > 维护 > License管理”。
    - 在“License激活方式”中选择“本地手动激活”。
    - 单击“浏览”，选择待上传的License文件。
    - 单击“激活”，激活当前License文件。



目录



VRP命令行级别

级别	说明
参观级	网络诊断工具命令（ping、tracert）、从本设备出发访问外部设备的命令（包括：Telnet客户端、SSH、Rlogin）等，该级别命令不允许进行配置文件保存的操作。
监控级	用于系统维护、业务故障诊断等，包括display、debugging命令，该级别命令不允许进行配置文件保存的操作。
配置级	业务配置命令，包括路由、各个网络层次的命令，这些用于向用户提供直接网络服务。
管理级	关系到系统基本运行，系统支撑模块的命令，这些命令对业务提供支撑作用

 Page 53



VRP系统命令采用分级保护方式，命令被划分为参观级、监控级、配置级、管理级4个级别。

参观级：网络诊断工具命令（ping、tracert）、从本设备出发访问外部设备的命令（包括：Telnet客户端、SSH、Rlogin）等，该级别命令不允许进行配置文件保存的操作。

监控级：用于系统维护、业务故障诊断等，包括display、debugging命令，该级别命令不允许进行配置文件保存的操作。

配置级：业务配置命令，包括路由、各个网络层次的命令，这些用于向用户提供直接网络服务。

管理级：关系到系统基本运行，系统支撑模块的命令，这些命令对业务提供支撑作用，包括文件系统、FTP、TFTP、Xmodem下载、配置文件切换命令、备板控制命令、用户管理命令、命令级别设置命令、系统内部参数设置命令等。

系统对登录用户也划分为4级，分别与命令级别对应，即不同级别的用户登录后，只能使用等于或低于自己级别的命令。当用户从低级别用户切换到高级别用户时，需要使用命令：super password [level user-level] { simple | cipher } password 切换。

VRP命令视图

- 系统将命令行接口划分为若干个命令视图，系统的所有命令都注册在某个（或某些）命令视图下，只有在相应的视图下才能执行该视图下的命令。
- 命令视图的分类：
  - 用户视图
    - <USG>
  - 系统视图
    - [USG]
  - 接口视图
    - [USG -Ethernet0/0/1]
  - 协议视图
    - [USG -rip]
  - ……

 Page 54



系统将命令行接口划分为若干个命令视图，系统的所有命令都注册在某个（或某些）命令视图下，只有在相应的视图下才能执行该视图下的命令。

与防火墙建立连接即进入用户视图，它只完成查看运行状态和统计信息的简单功能，再键入system-view进入系统视图，在系统视图下，可以再键入不同的配置命令进入相应的协议、接口等视图。

VRP在线帮助

- 键入一命令，后接以空格分隔的“?”，如果该位置为关键字，则列出全部关键字及其简单描述。

  <USG 5000> display ?

- 键入一命令，后接以空格分隔的“?”，如果该位置为参数，则列出有关的参数描述。

  [USG 5000] interface ethernet ?

  <3-3> Slot number

- 键入一字符串，其后紧接“?”，列出以该字符串开头的所有命令。

  <USG 5000> d?

  debugging delete dir display



VRP平台提供十分方便的命令行在线帮助，只需要在有疑问的地方键入问号即可。

例如在系统视图下直接键入问号，系统便会列出在系统视图下可以配置的命令参数，或者在参数后键入空格，然后再键入问号，便可获得该参数后可以使用的参数列表，如果是键入一字符串，其后紧接键入问号，则系统会列出以该字符串开头的所有命令。

VRP在线帮助（续）

- 输入命令的某个关键字的前几个字母，按下<TAB>键，可以显示出完整的关键字
- 暂停显示时键入<Ctrl+C>　停止显示和命令执行
- 暂停显示时键入空格键　　继续显示下一屏信息
- 暂停显示时键入回车键　　继续显示下一行信息



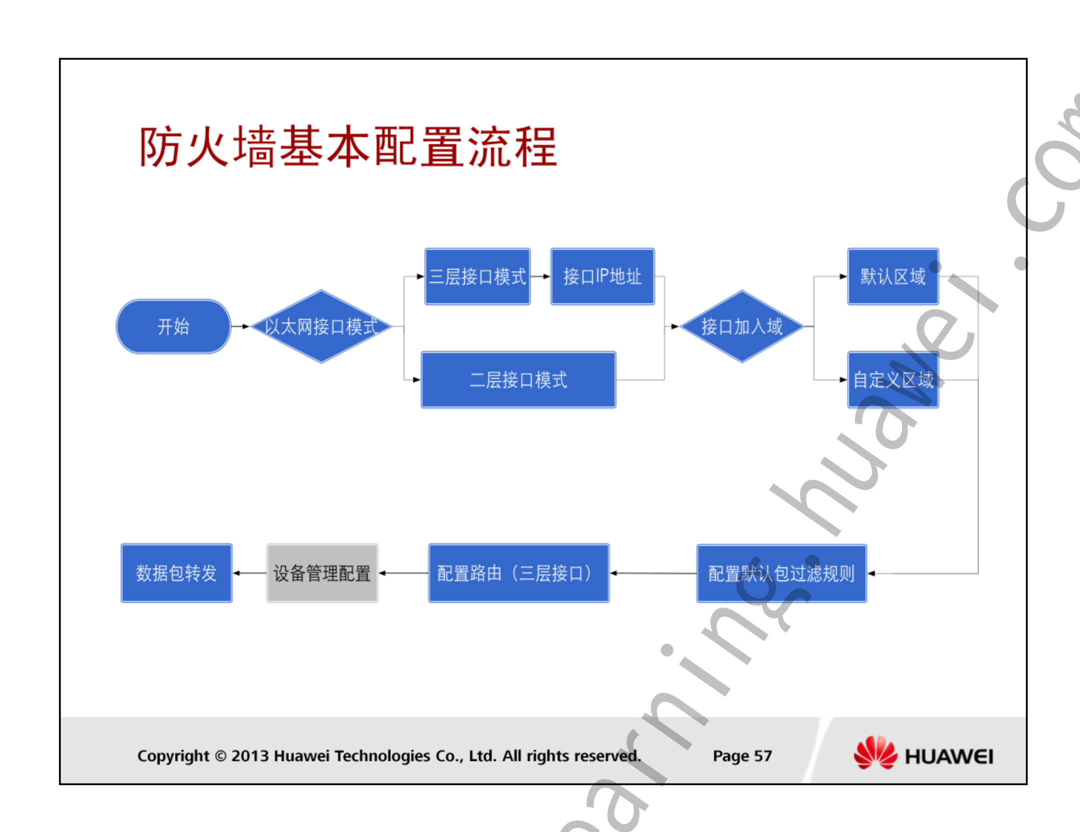
输入命令的某个关键字的前几个字母，按下<tab>键，系统还可以显示出完整的关键字。

我们看到有的时候在一次显示信息有可能会超过一屏，此时系统提供了暂停功能，这时用户可以有三种选择：

暂停显示时键入<Ctrl+c>　停止显示和命令执行

暂停显示时键入空格键　　继续显示下一屏信息

暂停显示时键入回车键　　继续显示下一行信息



以上配置流程不等同于防火墙转发流程。

基本配置包括基本功能配置和设备管理配置。

配置接口模式

步骤 1 进入系统视图。

<USG>system-view

步骤 2 进入接口视图

[USG]interface interface-type interface-number

步骤 3 配置三层以太网接口或者二层以太网接口

配置三层以太网接口

ip address ip-address { mask | mask-length }，。

或配置二层以太网接口

portswitch



在USG中，支持以下两种接口卡：

二层接口卡：所有接口均为二层以太网接口，不支持切换为三层接口。

三层接口卡：所有接口缺省为三层以太网接口，可以通过命令portswitch切换为二层以太网接口。

配置安全区域

步骤 1 执行命令**system-view**，进入系统视图。

步骤 2 执行命令**firewall zone** [**vpn-instance** *vpn-instance-name*] [**name**] *zone-name*，创建安全区域，并进入相应安全区域视图。

安全区域已经存在	不必配置关键字name，直接进入安全区域视图
安全区域不存在	需要配置关键字name，进入安全区域视图

步骤 3 执行命令**set priority** *security-priority*，配置安全区域的安全级别。

Page 59



- 创建自定义安全区域。

步骤1 执行命令system-view，进入系统视图。

步骤2 执行命令firewall zone [vpn-instance vpn-instance-name] [name] zone-name，创建安全区域，并进入相应安全区域视图。

执行firewall zone命令时，存在如下两种情况：

安全区域已经存在：不必配置关键字name，直接进入安全区域视图。

安全区域不存在：需要配置关键字name，进入安全区域视图。

系统预定义了Local、Trust、DMZ、Untrust 共4个安全区域。在路由模式下，4个安全区域无需创建，也不能删除。防火墙最多支持16个安全区域

步骤3 执行命令set priority security-priority，配置安全区域的安全级别。

- 配置安全区域的安全级别时，需要遵循如下原则：

1. 只能为自定义的安全区域设定安全级别。

2. 安全级别一旦设定，不允许更改。

3. 同一系统中，两个安全区域不允许配置相同的安全级别。

4. 新建的安全区域，未设定其安全级别前，系统规定其安全级别为0。

将接口加入安全区域

步骤 1 执行命令**system-view**，进入系统视图。

步骤 2 执行命令**firewall zone** [**vpn-instance** *vpn-instance-name*] [**name**] *zone-name*，创建安全区域，并进入相应安全区域视图。

步骤 3 执行命令**add interface** *interface-type interface-number*，配置接口加入安全区域。



配置域间缺省包过滤规则

步骤 1 执行命令system-view，进入系统视图。

步骤 2 执行命令firewall packet-filter default { permit | deny } { { all | interzone zone1 zone2 } [direction { inbound | outbound }] }，配置域间缺省包过滤规则。



zone1与zone2有先后顺序吗？？？

没有先后顺序。因为Inbound和Outbound的方向只与域的优先级有关



- 配置域间包过滤规则

当数据流无法匹配防火墙中的ACL时，会按照域间缺省包过滤规则转发或丢弃该数据流的报文。配置域间缺省包过滤规则，需要进行如下操作。

步骤 1 执行命令system-view，进入系统视图。

步骤 2 执行命令firewall packet-filter default { permit | deny } { { all | interzone zone1 zone2 } [direction { inbound | outbound }] }，配置域间缺省包过滤规则。

参数说明：

permit：默认过滤规则为允许；deny：默认过滤规则为禁止；all：配置作用于所有安全区域间；interzone：配置作用于特定安全区域间；zone1：第一个安全区域的名字，可以是DMZ、Local、Trust、Untrust区域以及自定义区域；zone2：第二个安全区域的名字，可以是DMZ、Local、Trust、Untrust区域以及自定义区域；direction：配置过滤规则作用的方向；inbound：配置过滤规则作用于安全区域间入方向；outbound：配置过滤规则作用于安全区域间出方向。

缺省情况下，在防火墙所有安全区域间的所有方向都禁止报文通过。

配置路由

- 配置静态路由，需要进行如下操作。

  步骤 1 执行命令**system-view**，进入系统视图。

  步骤 2 执行命令**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-ip-address* } [**preference** *value*] [**reject** | **blackhole**]增加一条静态路由

- 配置缺省路由，需要进行如下操作。

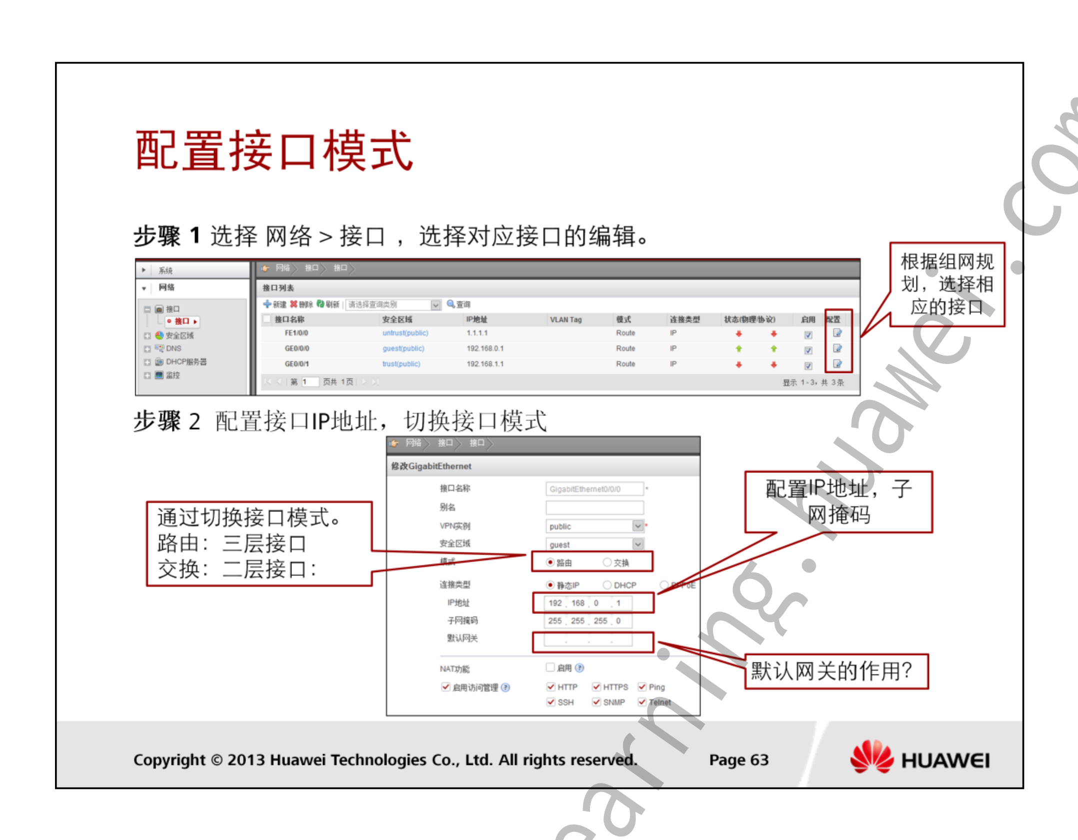
  步骤 1 执行命令**system-view**，进入系统视图。

  步骤 2 执行命令**ip route-static 0.0.0.0** { **0.0.0.0** | **0** } { *interface-type interface-number* | next-ip-*address* } [**preference** *value*] [**reject** | **blackhole**]，配置缺省路由。

 Page 62 

通过静态路由的配置可建立一个互通的网络，但这种配置问题在于：当一个网络故障发生后，静态路由不会自动发生改变，必须有管理员的介入。

缺省路由就是在没有找到匹配的路由表入口项时才使用的路由。即只有当没有合适的路由时，缺省路由才被使用。在路由表中，缺省路由以到网络0.0.0.0（掩码为0.0.0.0）的路由形式出现。如果报文的目的地址不能与路由表的任何入口项相匹配，那么该报文将选取缺省路由。如果没有缺省路由且报文的目的地不在路由表中，那么该报文被丢弃的同时，将向源端返回一个ICMP 报文报告该目的地址或网络不可达。



步骤 1 选择 网络 > 接口 ，选择对应接口的编辑

步骤 2 配置接口IP地址，切换接口模式

在USG中，支持以下两种接口卡：

二层接口卡：所有接口均为二层以太网接口，不支持切换为三层接口。

三层接口卡：所有接口缺省为三层以太网接口，可以通过命令portswitch切换为二层以太网接口。

将接口加入安全区域 （1）

步骤 1 选择网络 > 接口 > 接口。

步骤 2 选择新建区域或者默认区域

步骤 3 如果新建区域，配置区域名称和安全级别。



 Page 64 

步骤 1 选择网络 > 接口 > 接口。

步骤 2 选择新建区域或者默认区域。

步骤 3 如果新建区域，配置区域名称和安全级别。

将接口加入安全区域 （2）

步骤 4 将接口加入安全区域

网络 > 安全区域 > 安全区域

修改安全区域

安全区域名称 guest *

优先级 10 *<1-100>

描述

应用 返回

将接口通过“添加”按钮，添加到域中。

未加入域的接口
刷新 请选择接口类型 查询 添加
接口名称
FE1/0/0
GE0/0/1

已加入域的接口
删除 刷新 请选择接口类型 查询
接口名称
GE0/0/0

如果你想添加的接口，未出现在未加入域的接口列表中，是什么原因？ 如何解决。



步骤 4 将接口加入安全区域

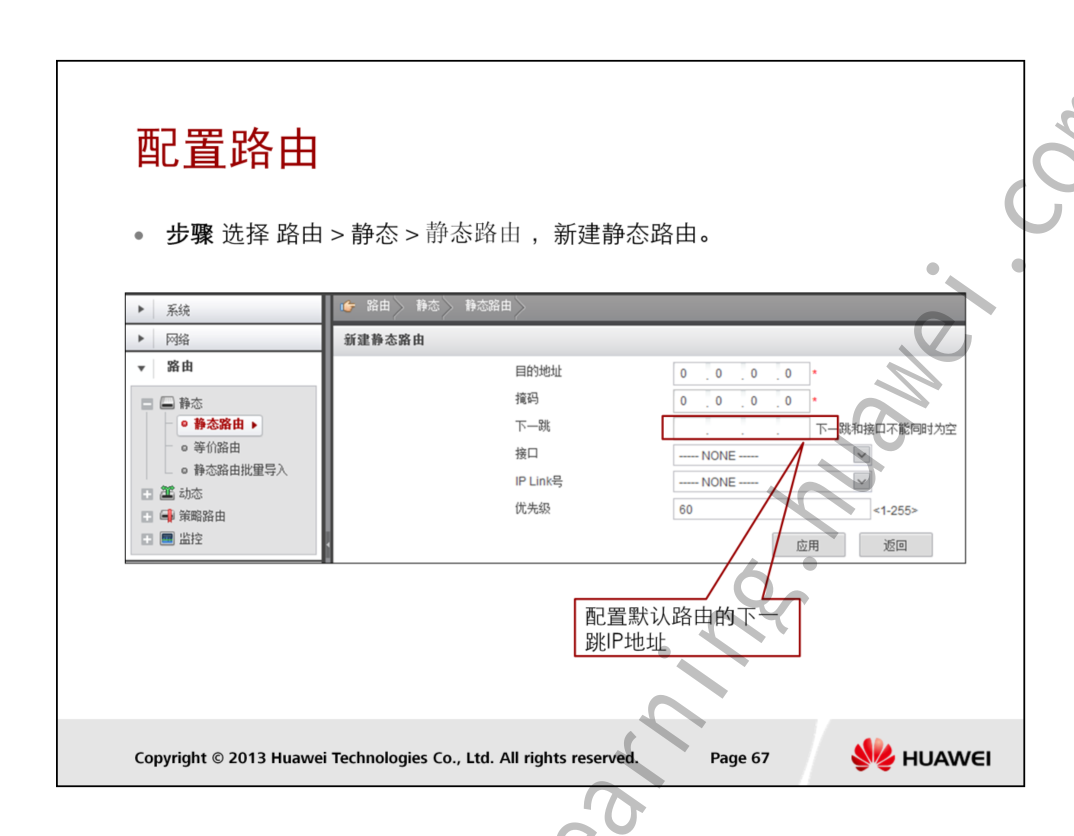
配置域间缺省包过滤规则

- **步骤** 选择 防火墙 > 安全策略 > 转发策略 ， 选择对应的域间编辑按钮。



- **配置域间包过滤规则**

  步骤 选择 防火墙 > 安全策略 > 转发策略 ， 选择对应的域间编辑按钮。



步骤 选择 路由 > 静态 > 静态路由 ， 新建静态路由。



总结

- 防火墙的定义和分类
- 防火墙的主要功能和技术
- 防火墙设备管理
- 防火墙的基本配置



思考题

- 状态检测防火墙与包过滤防火墙有哪些不同?
- 安全区域与接口之间有哪些关系?
- Inbound和Outbound在域间包过滤策略中有何不同?
- 可靠性技术IP LINK与静态路由和双机热备整合后，有哪些优势?

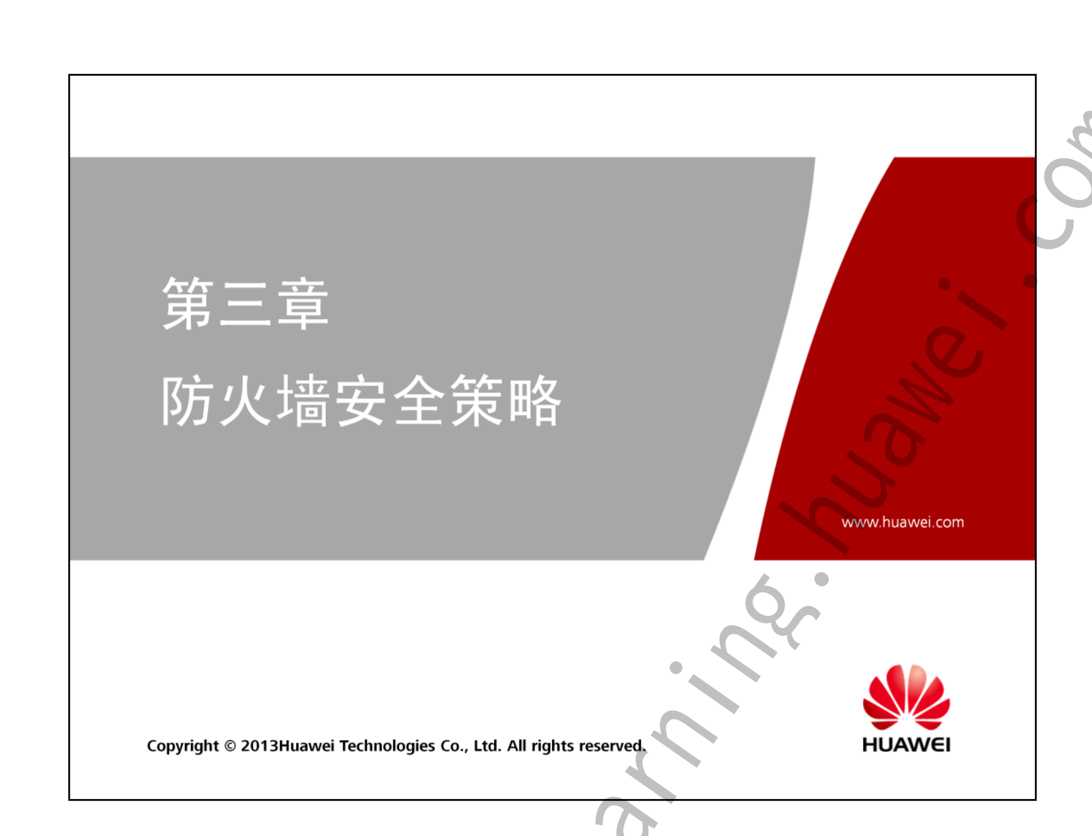


Thank you

www.huawei.com

HC110310003

HCNA-Security-CBSN 第三章 防火墙安全策略


第三章
防火墙安全策略
www.huawei.com
Copyright © 2013Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目标

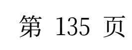
- 学完本课程后，您将能够:
  - 理解防火墙包过滤技术
  - 理解防火墙转发原理
  - 理解防火墙安全策略
  - 掌握防火墙安全策略配置

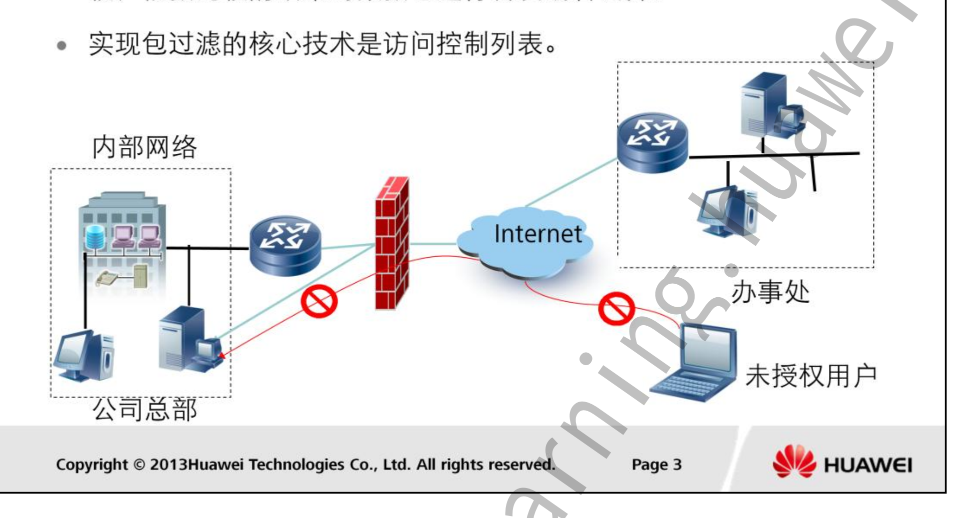




目录



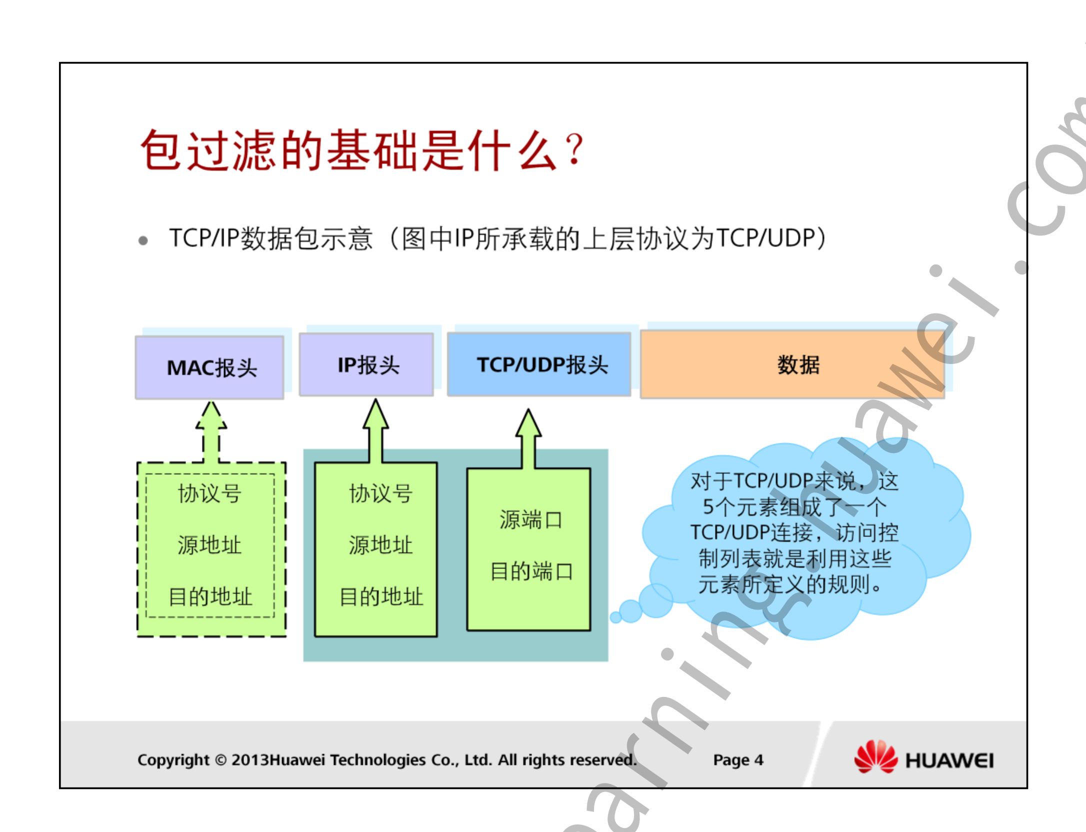




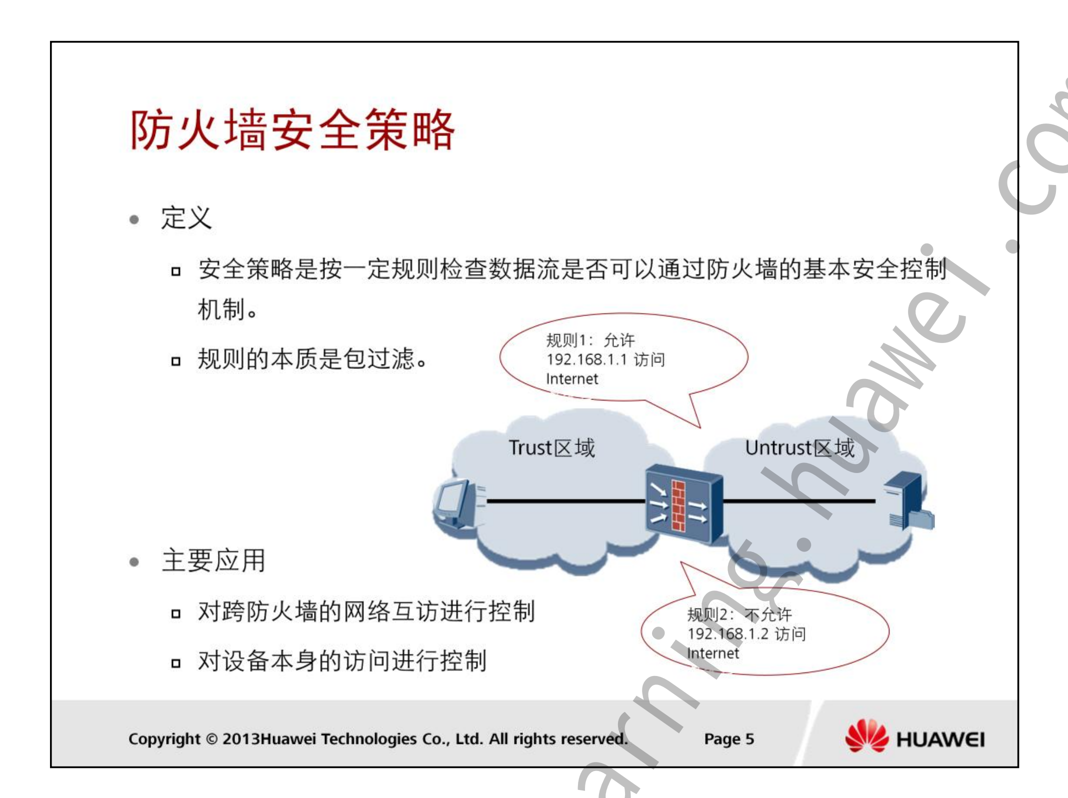
包过滤作为一种网络安全保护机制，主要用于对网络中各种不同的流量是否转发做一个最基本的控制。

传统的包过滤防火墙对于需要转发的报文，会先获取报文头信息，包括报文的源IP地址、目的IP地址、IP层所承载的上层协议的协议号、源端口号和目的端口号等，然后和预先设定的过滤规则进行匹配，并根据匹配结果对报文采取转发或丢弃处理。

包过滤防火墙的转发机制是逐包匹配包过滤规则并检查，所以转发效率低下。目前防火墙基本使用状态检查机制，将只对一个连接的首包进行包过滤检查，如果这个首包能够通过包过滤规则的检查，并建立会话的话，后续报文将不再继续通过包过滤机制检测，而是直接通过会话表进行转发。

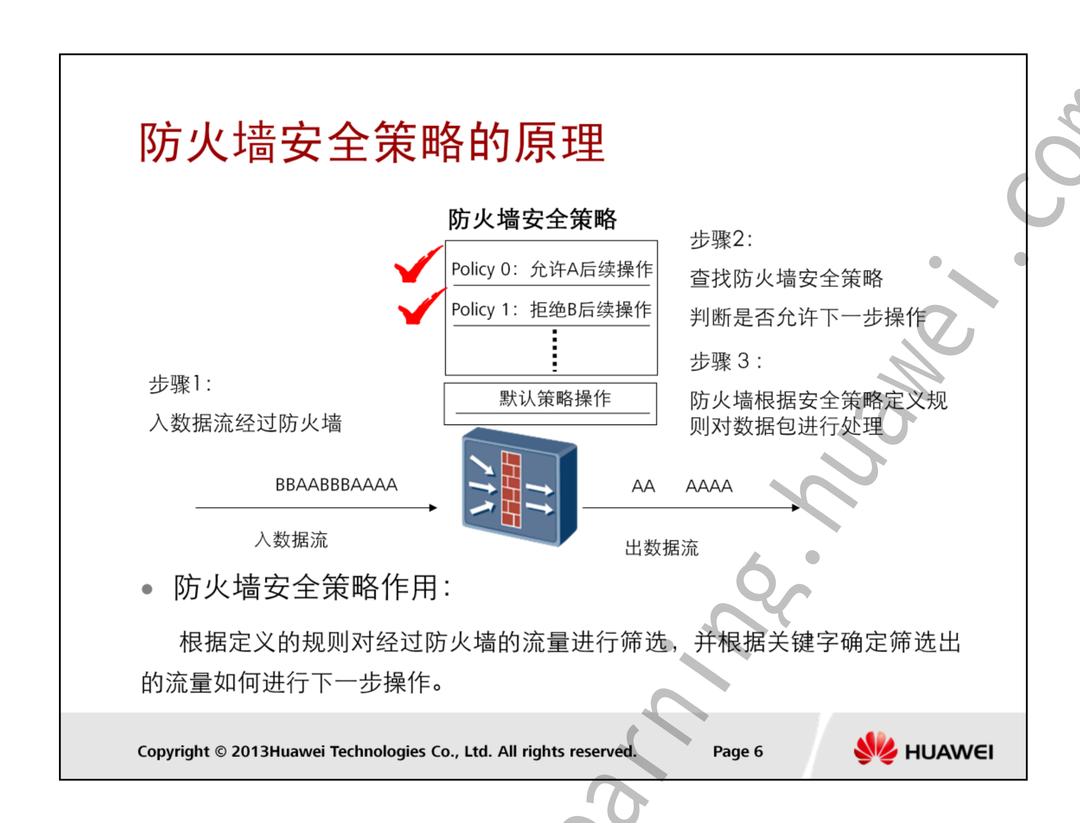


包过滤能够通过报文的源MAC地址、目的MAC地址、源IP地址、目的IP地址、源端口号、目的端口号、上层协议等信息组合定义网络中的数据流，其中源IP地址、目的IP地址、源端口号、目的端口号、上层协议就是在状态检测防火墙中经常所提到的五元组，也是组成TCP/UDP连接非常重要的五个元素。



防火墙的基本作用是保护特定网络免受“不信任”的网络的攻击，但是同时还必须允许两个网络之间可以进行合法的通信。安全策略的作用就是对通过防火墙的数据流进行检验，符合安全策略的合法数据流才能通过防火墙。

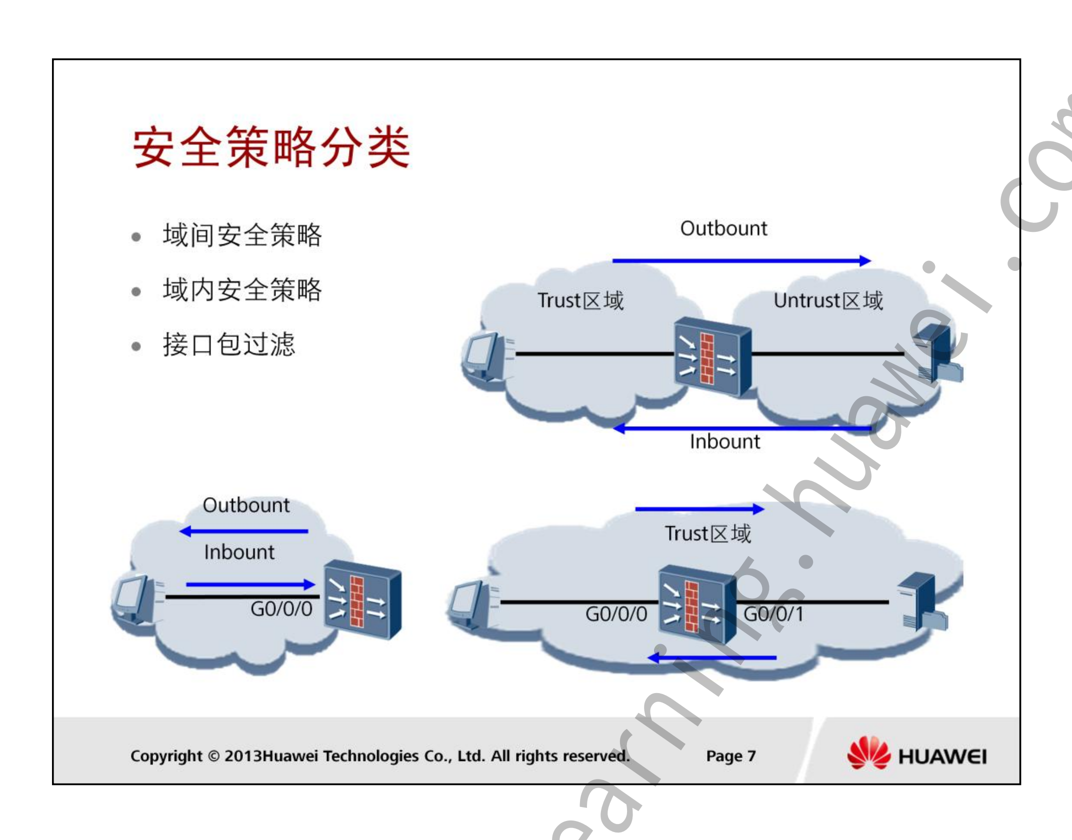
通过防火墙安全策略可以控制内网访问外网的权限、控制内网不同安全级别的子网间的访问权限等。同时也能够对设备本身的访问进行控制，例如限制哪些IP地址可以通过Telnet和Web等方式登录设备，控制网管服务器、NTP服务器等与设备的互访等。



防火墙安全策略定义数据流在防火墙上的处理规则，防火墙根据规则对数据流进行处理。因此，防火墙安全策略的核心作用是：根据定义的规则对经过防火墙的流量进行筛选，由关键字确定筛选出的流量如何进行下一步操作。

在防火墙应用中，防火墙安全策略是对经过防火墙的数据流进行网络安全访问的基本手段，决定了后续的应用数据流是否被处理。安全策略根据通过报文的源地址、目的地址、端口号、上层协议等信息组合定义网络中的数据流。

思考：五元组在安全策略中是如何进行匹配的？



域间安全策略用于控制域间流量的转发（此时称为转发策略），适用于接口加入不同安全区域的场景。域间安全策略按IP地址、时间段和服务（端口或协议类型）、用户等多种方式匹配流量，并对符合条件的流量进行包过滤控制（permit/deny）或高级的UTM应用层检测。域间安全策略也用于控制外界与设备本身的互访（此时称为本地策略），按IP地址、时间段和服务（端口或协议类型）等多种方式匹配流量，并对符合条件的流量进行包过滤控制（permit/deny），允许或拒绝与设备本身的互访。

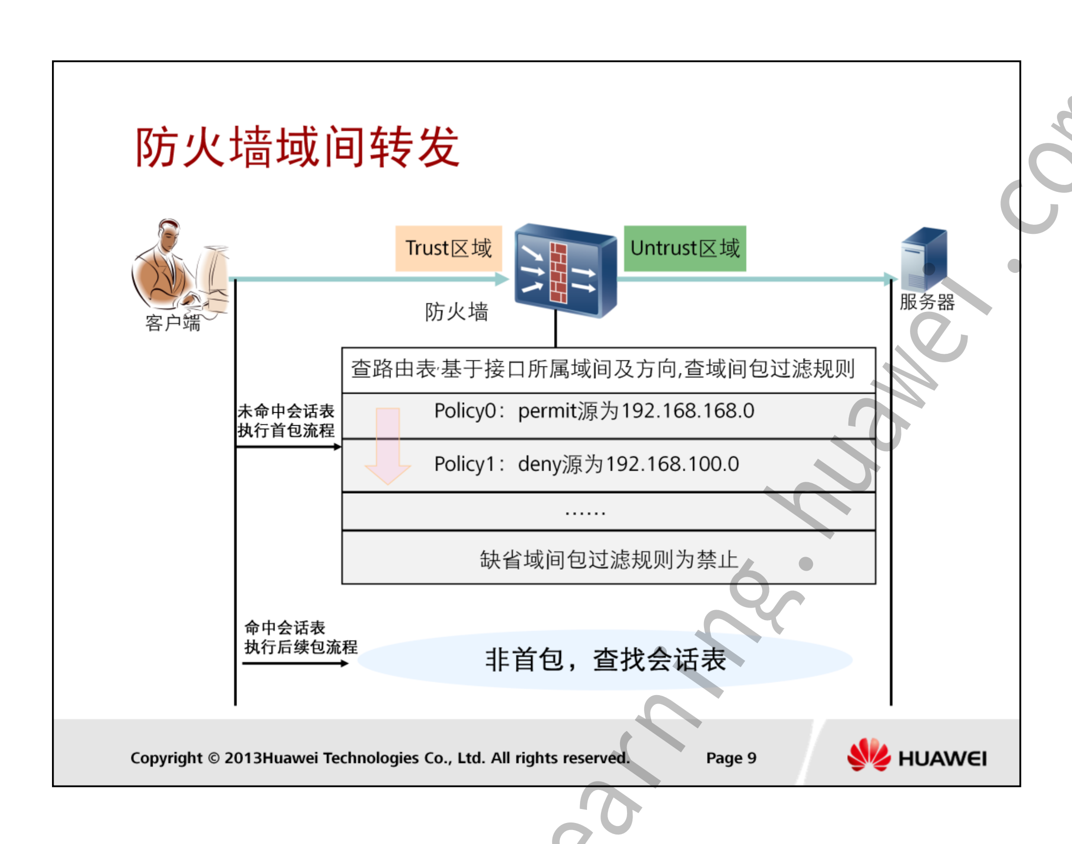
缺省情况下域内数据流动不受限制，如果需要进行安全检查可以应用域内安全策略。与域间安全策略一样可以按IP地址、时间段和服务（端口或协议类型）、用户等多种方式匹配流量，然后对流量进行安全检查。例如：市场部和财务部都属于内网所在的安全区域Trust，可以正常互访。但是财务部是企业重要数据所在的部门，需要防止内部员工对服务器、PC等的恶意攻击。所以在域内应用安全策略进行IPS检测，阻断恶意员工的非法访问。

当接口未加入安全区域的情况下，通过接口包过滤控制接口接收和发送的IP报文，可以按IP地址、时间段和服务（端口或协议类型）等多种方式匹配流量并执行相应动作（permit/deny）。基于MAC地址的包过滤用来控制接口可以接收哪些以太网帧，可以按MAC地址、帧的协议类型和帧的优先级匹配流量并执行相应动作（permit/deny）。硬件包过滤是在特定的二层硬件接口卡上实现的，用来控制接口卡上的接口可以接收哪些流量。硬件包过滤直接通过硬件实现，所以过滤速度更快。



目录



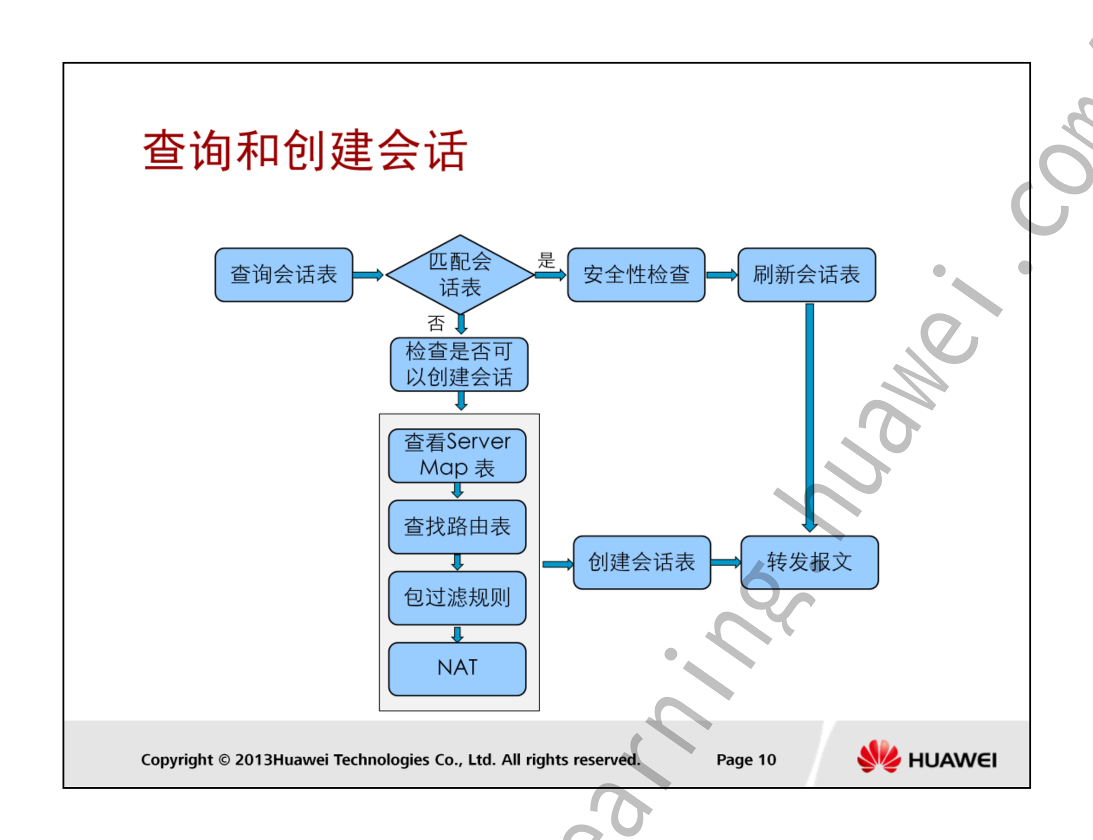


早期包过滤防火墙采取的是“逐包检测”机制，即对设备收到的所有报文都根据包过滤规则每次都进行检查以决定是否对该报文放行。这种机制严重影响了设备转发效率，使包过滤防火墙成为网络中的转发瓶颈。

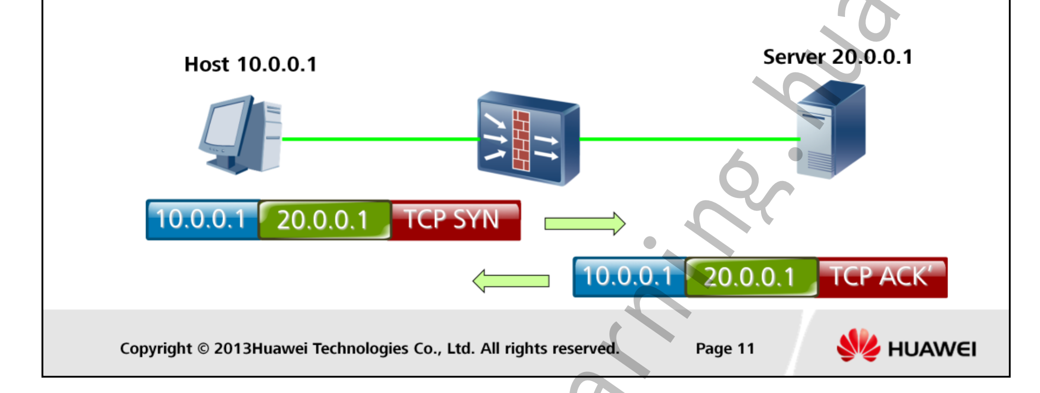
于是越来越多的防火墙产品采用了“状态检测”机制来进行包过滤。“状态检测”机制以流量为单位来对报文进行检测和转发，即对一条流量的第一个报文进行包过滤规则检查，并将判断结果作为该条流量的“状态”记录下来。对于该流量的后续报文都直接根据这个“状态”来判断是转发还是丢弃，而不会再次检查报文的数据内容。这个“状态”就是我们平常所述的会话表项。这种机制迅速提升了防火墙产品的检测速率和转发效率，已经成为目前主流的包过滤机制。

在防火墙一般是检查IP报文中的五个元素，又称为“五元组”，即源IP地址和目的IP地址，源端口号和目的端口号，协议类型。通过判断IP数据报文报文的五元组，就可以判断一条数据流相同的IP数据报文。

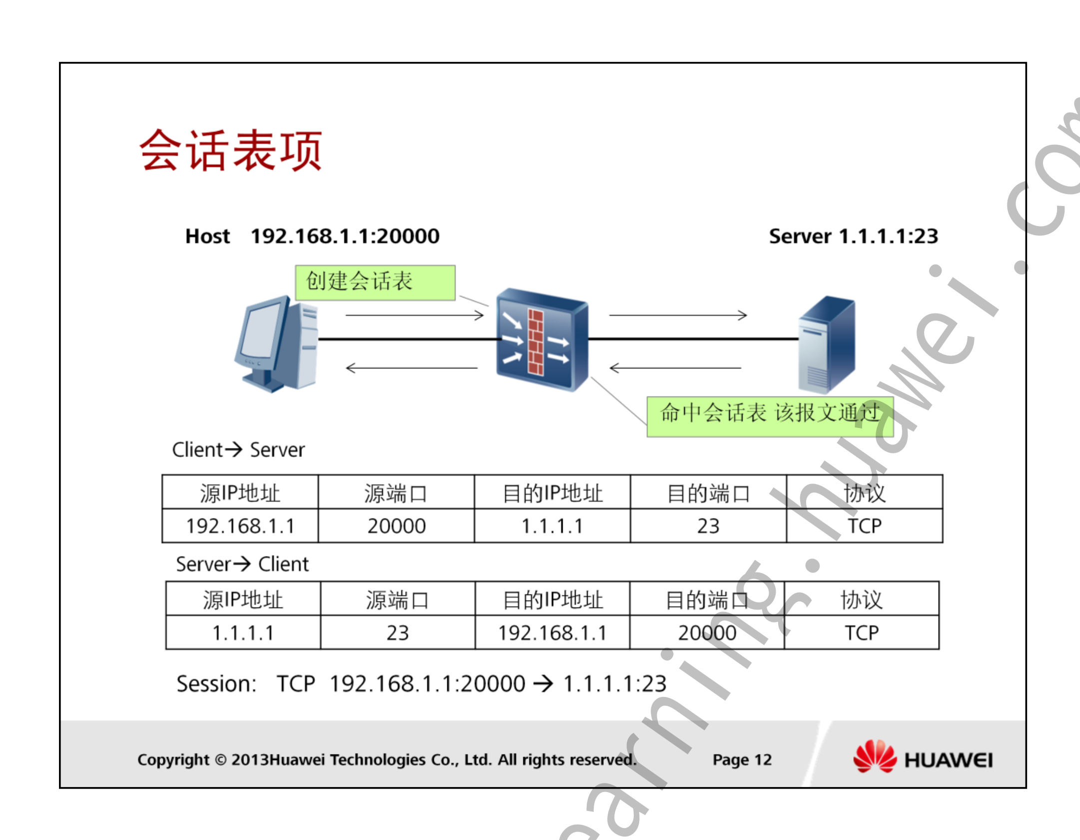
其中TCP协议的数据报文，一般情况下在三次握手阶段除了基于五元组外，还会计算及检查其它字段。三次握手建立成功后，就通过会话表中的五元组对设备收到后续报文进行匹配检测，以确定是否允许此报文通过。



可以看出，对于已经存在会话表的报文的检测过程比没有会话表的报文要短很多。而通常情况下，通过对一条连接的首包进行检测并建立会话后，该条连接的绝大部分报文都不再需要重新检测。这就是状态检测防火墙的“状态检测机制”相对于包过滤防火墙的“逐包检测机制”的改进之处。这种改进使状态检测防火墙在检测和转发效率上有迅速提升。



- 对于TCP报文
  - 开启状态检测机制时，首包（SYN报文）建立会话表项。对除SYN报文外的其他报文，如果没有对应会话表项（设备没有收到SYN报文或者会话表项已老化），则予以丢弃，也不会建立会话表项。
  - 关闭状态检测机制时，任何格式的报文在没有对应会话表项的情况下，只要通过各项安全机制的检查，都可以为其建立会话表项。
- 对于UDP报文
  - UDP是基于无连接的通信，任何UDP格式的报文在没有对应会话表项的情况下，只要通过各项安全机制的检查，都可以为其建立会话表项。
- 对于ICMP报文
  - 开启状态检测机制时，没有对应会话的ICMP应答报文将被丢弃。
  - 关闭状态检测机制时，没有对应会话的应答报文以首包形式处理



会话是状态检测防火墙的基础，每一个通过防火墙的数据流都会在防火墙上建立一个会话表项，以五元组（源目的IP地址、源目的端口、协议号）为Key值，通过建立动态的会话表提供域间转发数据流更高的安全性。

- 会话表包括五个元素：
  - 源IP地址
  - 源端口
  - 目的IP地址
  - 目的端口
  - 协议号

查看会话表信息

<USG> **display firewall session table verbose**

Current total sessions: 1

icmp VPN: public --> public

Zone: trust --> untrust Slot: 8 CPU: 0 TTL: 00:00:20 Left: 00:00:19

Interface: GigabitEthernet6/0/0 Nexthop: 107.255.255.10

<--packets: 134 bytes: 8040 -->packets: 134 bytes: 8040

107.229.15.100:1280 --> 107.228.10.100:2048

 Page 13



display firewall session table [verbose]

用来显示系统当前的会话表项信息，verbose参数来控制是否显示详细的信息。

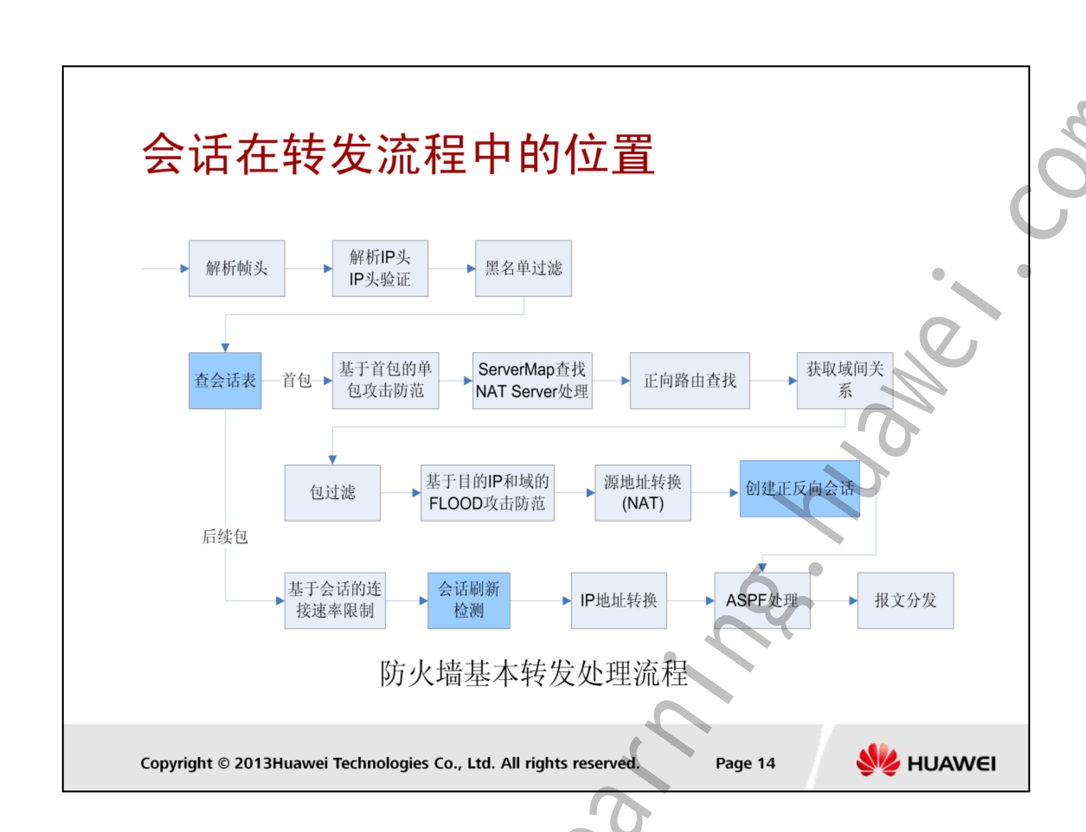
- icmp 表示会话表的应用类型为ICMP协议。
- trust --> untrust 表示从Trust区域到Untrust区域方向的流量建立的会话。
- Interface 表示流量的入接口。
- Nexthop 表示流量的下一跳地址。
- <--packets 表示反向报文命中的会话数，即从Untrust到Trust方向的报文数。

说明： 在NAT或VPN应用中，反向会话的报文统计数通常会有延时。

- -->packets 表示正向报文命中的会话数，即从Trust到Untrust方向的报文数。
- 107.229.15.100:1280 表示源IP地址和源端口
- 107.228.10.100:2048 表示目的IP地址和目的端口

<USG> reset firewall session table

- 清除系统当前会话表项。
- Reset Session表项操作得谨慎，因为会导致在运行业务中断。



当防火墙收到报文后，根据五元组信息查询会话表，并根据具体情况进行操作。

多通道协议技术

- 单通道协议：通信过程中只需占用一个端口的协议。如：WWW只需占用80端口
- 多通道协议：通信过程中需占用两个或两个以上端口的协议。如FTP被动模式下需占用21号端口以及一个随机端口

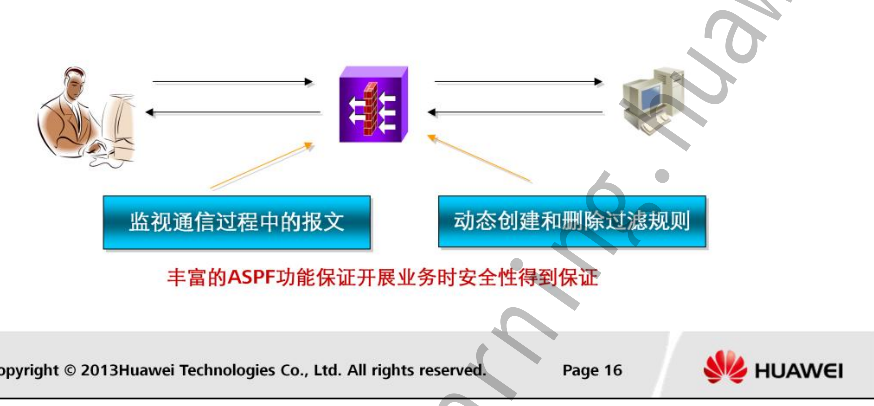
使用单纯的包过滤方法，如何精确定义（端口级别）多通道协议所使用的端口呢？

遇到使用随机协商端口的协议，单纯的包过滤方法无法进行数据流定义。

 Page 15



大部分多媒体应用协议（如H.323、SIP）、FTP、netmeeting等协议使用约定的固定端口来初始化一个控制连接，再动态的选择端口用于数据传输。端口的选择是不可预测的，其中的某些应用甚至可能要同时用到多个端口。传统的包过滤防火墙可以通过配置ACL过滤规则匹配单通道协议的应用传输，保障内部网络不受攻击，但只能阻止一些使用固定端口的应用，无法匹配使用协商出随机端口传输数据的多通道协议应用，留下了许多安全隐患。



ASPF在session表的数据结构中维护着连接的状态信息，并利用这些信息来维护会话的访问规则。ASPF保存着不能由访问控制列表规则保存的重要的状态信息。防火墙检验数据流中的每一个报文，确保报文的状态与报文本身符合用户所定义的安全规则。连接状态信息用于智能的允许/禁止报文。当一个会话终止时，session表项也将被删除，防火墙中的会话也将被关闭。

ASPF可以智能的检测“TCP的三次握手的信息”和“拆除连接的握手信息”，通过检测握手、拆连接的状态检测，保证一个正常的TCP访问可以正常进行，而对于非完整的TCP握手连接的报文会直接拒绝。

UDP是无连接的报文，所以也没有真正的UDP“连接”。因为ASPF是基于连接的，它将对UDP报文的源、目的IP地址、端口进行检查，通过判断该报文是否与所设定的时间段内的其他UDP报文相类似，而近似判断是否存在一个连接。

在普通的场合，一般使用的是基于ACL的IP包过滤技术，这种技术比较简单，但缺乏一定的灵活性，在很多杂应用的场合普通包过滤是无法完成对网络的安全保护的。例如对于类似于应用FTP协议进行通信的多通道协议来说，配置防火墙则是非常困难的。

ASPF使防火墙能够支持一个控制连接上存在多个数据连接的协议，同时还可以在应用非常复杂的情况下方便的制订各种安全的策略。ASPF监听每一个应用的每一个连接所使用的端口，打开合适的通道让会话中的数据能够出入防火墙，在会话结束时关闭该通道，从而能够对使用动态端口的应用实施有效的访问控制。

ASPF对多通道协议的支持

- ASPF（Application Specific Packet Filter）是针对应用层的包过滤

Host 10.0.0.1

控 制 通 道

FTP Server
20.0.0.1

数 据 通 道

我使用4952端口与
你建立数据通道

Session表　FTP:10.0.0.1:4927 --> 20.0.0.1:21

FTP:10.0.0.1:4926 --> 20.0.0.1:4952

ServerMap 表

Inside-Address :Port	Global-Address :Port	Pro	AppType		TTL	Left
20.0.0.1 : 4952	---	tcp	FTP	DATA	00:01:00	00:00:47

　Page 17　HUAWEI

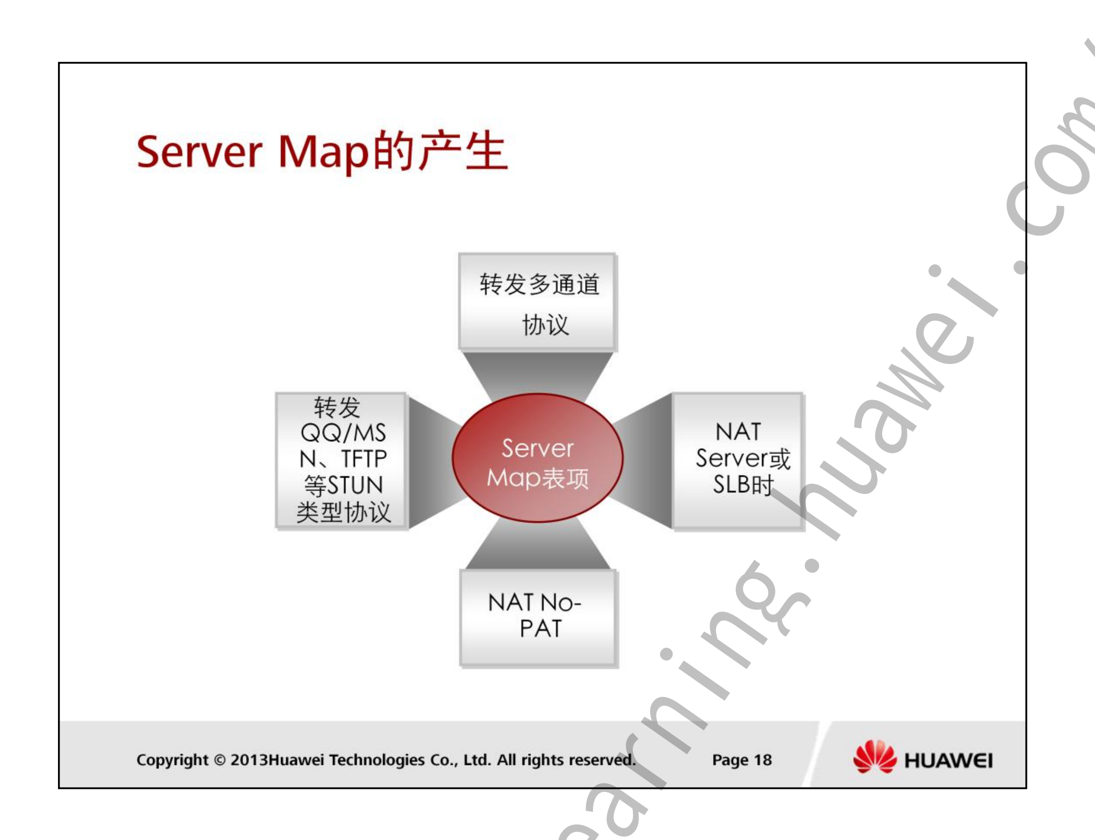
在多通道协议中，如FTP，控制通道和数据通道是分开的。数据通道是在控制报文中动态协商出来的，为了避免协商出来的通道不因其他规则的限制（如ACL）而中断，需要临时开启一个通道，Servermap就是为了满足这种应用而设计的一种数据结构。

FTP包含一个预知端口的TCP控制通道和一个动态协商的TCP数据通道，对于一般的包过滤防火墙来说，配置安全策略时无法预知数据通道的端口号，因此无法确定数据通道的入口，这样就无法配置准确的安全策略。ASPF技术则解决了这一问题，它检测IP层之上的应用层报文信息，并动态地根据报文的内容创建和删除临时的servermap表项，以允许相关的报文通过。

从图中可以看出，servermap表项是对FTP控制通道中动态检测过程中动态产生的，当报文通过防火墙时，ASPF将报文与指定的访问规则进行比较，如果规则允许，报文将接受检查，否则报文直接被丢弃。如果该报文是用于打开一个新的控制或数据连接，ASPF将动态的产生servermap表项，对于回来的报文只有是属于一个已经存在的有效的连接，才会被允许通过防火墙。在处理回来的报文时，状态表也需要更新。当一个连接被关闭或超时后，该连接对应的状态表将被删除，确保未经授权的报文不能随便透过防火墙。因此通过ASPF技术可以保证在应用复杂的情况下，依然可以非常精确的保证网络的安全。

Server-map是一种映射关系，当数据连接匹配了动态Server-map表项时，不需要再查找包过滤策略，保证了某些特殊应用的正常转发。另一种情况，当数据连接匹配Server-map表，会对报文中IP和端口进行转换。

Server-map通常只是用检查首个报文，通道建立后的报文还是根据会话表来转发。

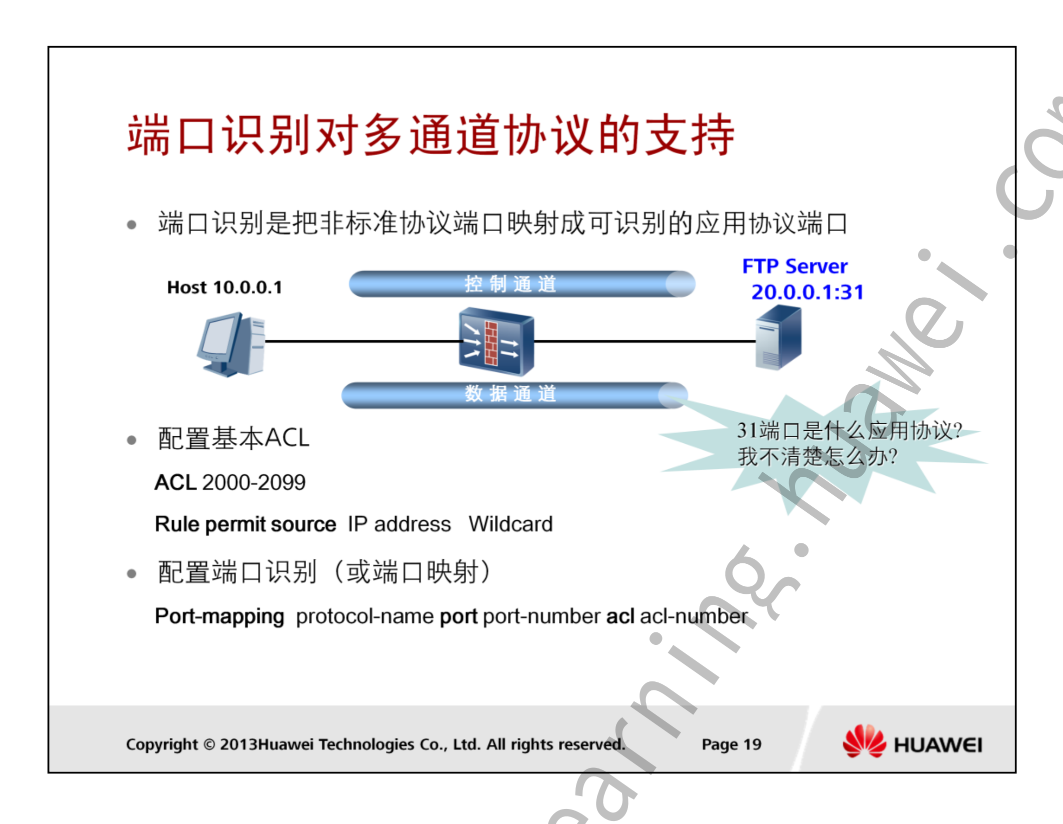


多通道协议会由客户端和服务器之间的控制通道动态协商出数据通道，即通信双方的端口号是不固定的。而在配置ASPF功能后，设备检测到控制通道的协商，根据关键报文载荷中的地址信息动态创建server-map表项，用于数据通道发起连接时进行查找。这个server-map表项包含了多通道协议报文中协商的数据通道的信息。

QQ/MSN等协议中，当用户登录之后，用户的IP地址和端口就固定下来了，可是会向该用户发起对话的另一方的IP地址和端口号是不固定的。通过配置STUN类型的ASPF，当QQ或者MSN等用户连接服务器时，设备会记录下用户的IP地址和端口信息，并动态生成STUN类型的Server-map。这个server-map表项中仅包含三元组信息，即通信一方的IP地址，端口号和协议号。这样其他用户可以直接通过该IP和端口与该用户进行通信。

在使用NAT Server功能时，外网的用户向内部服务器主动发起访问请求，该用户的IP地址和端口号都是不确定的，唯一可以确定的是内部服务器的IP地址和所提供服务的端口号。所以在配置NAT Server成功后，设备会自动生成Server-map表项，用于存放Globle地址与Inside地址的映射关系。设备根据这种映射关系对报文的地址进行转换并转发。每个生效的NAT Server都会生成正反方向两个静态的Server-map。在SLB功能中，由于需要将内网多个服务器以同一个IP地址对外发布，所以也会建立与NAT Server类似的Server-map表项，只不过根据内网服务器的个数需要建立1个正向表项和N个反向表项。

在使用NAT功能时，如果配置了No-PAT参数，那么设备会对内网IP和公网IP进行一对一的映射，而不进行端口转换。此时，内网IP的所有端口号都可以被映射为公网地址的对应端口，外网用户也就可以向内网用户的任意端口主动发起连接。所以配置NAT No-PAT后，设备会为有实际流量的数据流建立Server-map表，用于存放私网IP地址与公网IP地址的映射关系。设备根据这种映射关系对报文的地址进行转换，然后进行转发。



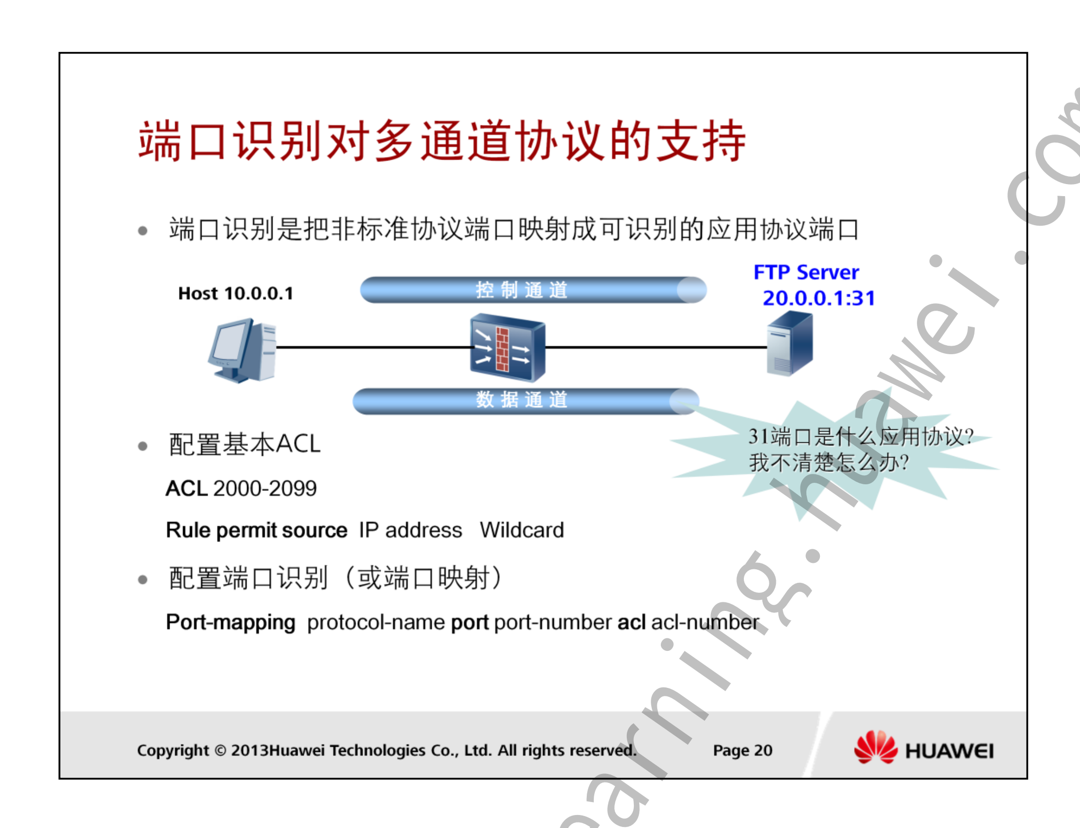
端口识别，也称端口映射，是防火墙用来识别使用非标准端口的应用层协议报文。端口映射支持的应用层协议包括FTP、HTTP、RTSP、PPTP、MGCP、MMS、SMTP、H323、SIP、SQLNET。

端口识别基于ACL进行，只有匹配某条ACL的报文，才会实施端口映射。端口映射使用基本ACL（编号2000～2999）。端口映射在使用ACL过滤报文时，使用报文的目的IP地址去匹配基本ACL中配置的源IP地址。

ACL(Access Control List),访问控制列表是一系列有顺序的规则组的集合，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL通过规则对数据包进行分类，这些规则应用到路由设备上，路由设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

ACL分为以下四类:

- 基本ACL（2000～2999）：只能通过源IP地址和时间段来进行流量匹配，在一些只需要进行简单匹配的功能可以使用。
- 高级ACL（3000～3999）：通过源IP地址、目的IP地址、ToS、时间段、协议类型、优先级、ICMP报文类型和ICMP报文码等多个维度来对进行流量匹配，在大部分功能中都可使用高级ACL来进行精确流量匹配。
- 基于MAC地址的ACL（4000～4999）：可以通过源MAC地址、目的MAC地址、CoS、协议码等维度来进行流量匹配。



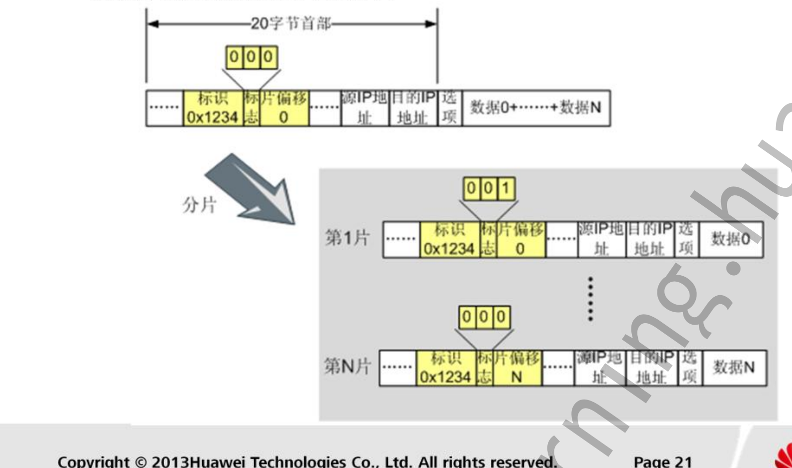
- 硬件包过滤ACL（9000～9499）：将硬件包过滤ACL下发到接口卡上后，接口卡通过硬件实现包过滤功能，比普通的软件包过滤速度更快，消耗系统资源更少。硬件包过滤ACL的匹配条件比较全面，可以通过源IP地址、目的IP地址、源MAC地址、目的MAC地址、CoS、协议类型等维度来进行流量匹配。

端口映射功能只对安全域间的数据流动生效，因此在配置端口映射时，也必须配置安全区域和安全域间。

思考：ACL所匹配的应用系统对象是什么？

分片缓存

- 分片缓存功能用来缓存先于首片分片报文到达的后续分片报文，避免分片报文被防火墙丢弃。





网络设备在传输报文时，如果设备上配置的MTU（Maximum Transfer Unit）小于报文长度，则会将报文分片后继续发送。理想情况下，各分片报文将按照固定的先后顺序在网络中传输。在实际传输过程中，可能存在首片分片报文不是第一个到达防火墙的现象。此时，防火墙将丢弃该系列分片报文。为保证会话的正常进行，缺省情况下，防火墙支持分片缓存功能。设备会将非首片的分片报文缓存至分片散列表，等待首片到来建立会话后，将所有分片报文进行转发。若在指定的时间内首片分片报文没有到来，防火墙将丢弃分片缓存中的分片报文。

在VPN应用中(如IPSEC和GRE)，由于需要设备对分片报文进行重组后解密或者解封装，设备才能进行后续处理，所以必须将设备配置成分片缓存状态，完成原始报文重组之后，才可以进行相应的加密解密处理。在NAT应用中，需要设备对分片报文进行重组后才能正常解析和转换报文中的IP地址，所以也必须将设备配置成分片缓存状态，才可以正常进行NAT。

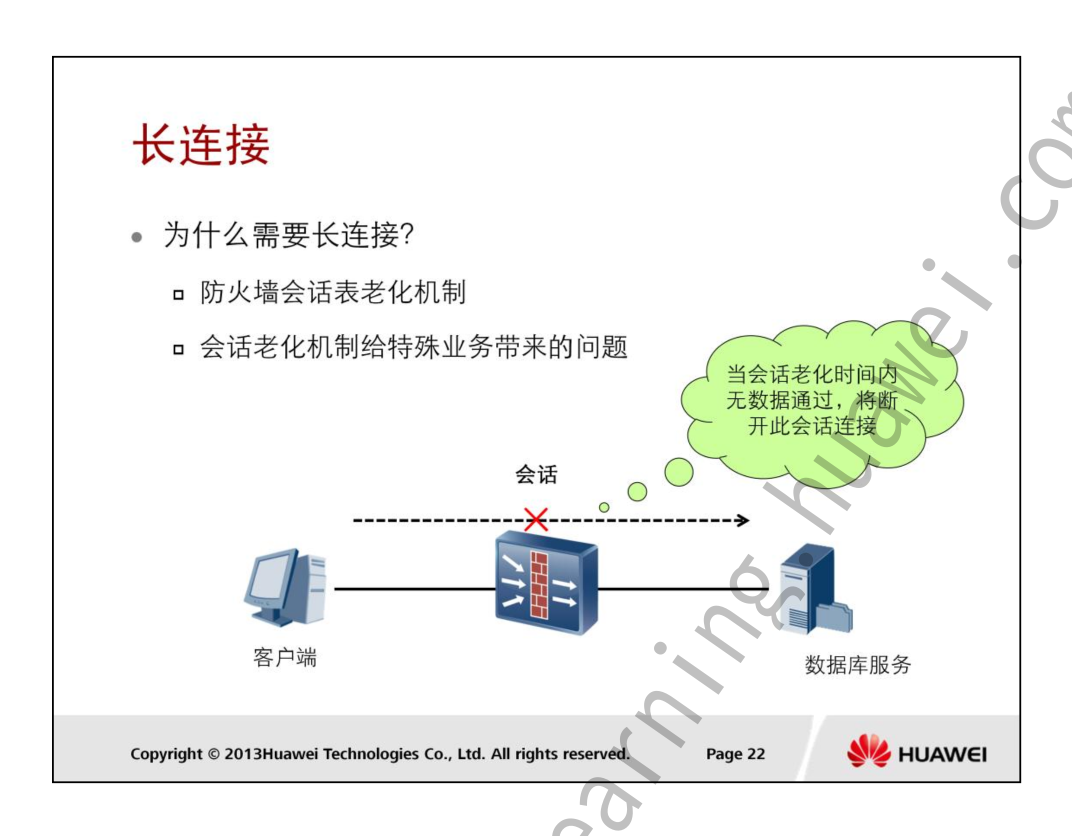
分片报文直接转发功能一般用在不进行NAT转换的情况下。开启该功能后，防火墙将收到的分片报文直接转发出去，不创建会话表。

- 配置分片缓存老化时间

  Firewall session aging-time fragment interval（1-40000）

- 开启/关闭分片报文直接转发功能

  Firewall fragment-forward enable/disable



当一个TCP会话的两个连续报文到达防火墙的时间间隔大于该会话的老化时间时，为保证网络的安全性，防火墙将从会话表中删除相应会话信息。这样，后续报文到达防火墙后，防火墙将丢弃该报文，导致连接中断。在实际的网络环境中，某些特殊的业务数据流的会话信息需要长时间不被老化。为了解决这一问题，防火墙支持在安全域间配置长连接功能，通过引用ACL定义数据流规则，为匹配ACL规则的特定报文的会话设置超长老化时间，确保会话正常进行。缺省情况下，长连接的老化时间为168小时（7*24小时）。

防火墙仅支持对TCP协议报文配置域间长连接功能。

状态检测机制关闭时，非首包也可以建立会话表，所以此时不需使用长连接功能也可保持业务的正常运行。

- 配置长连接老化时间

  Firewall long-link aging-time time

- 开启长连接功能

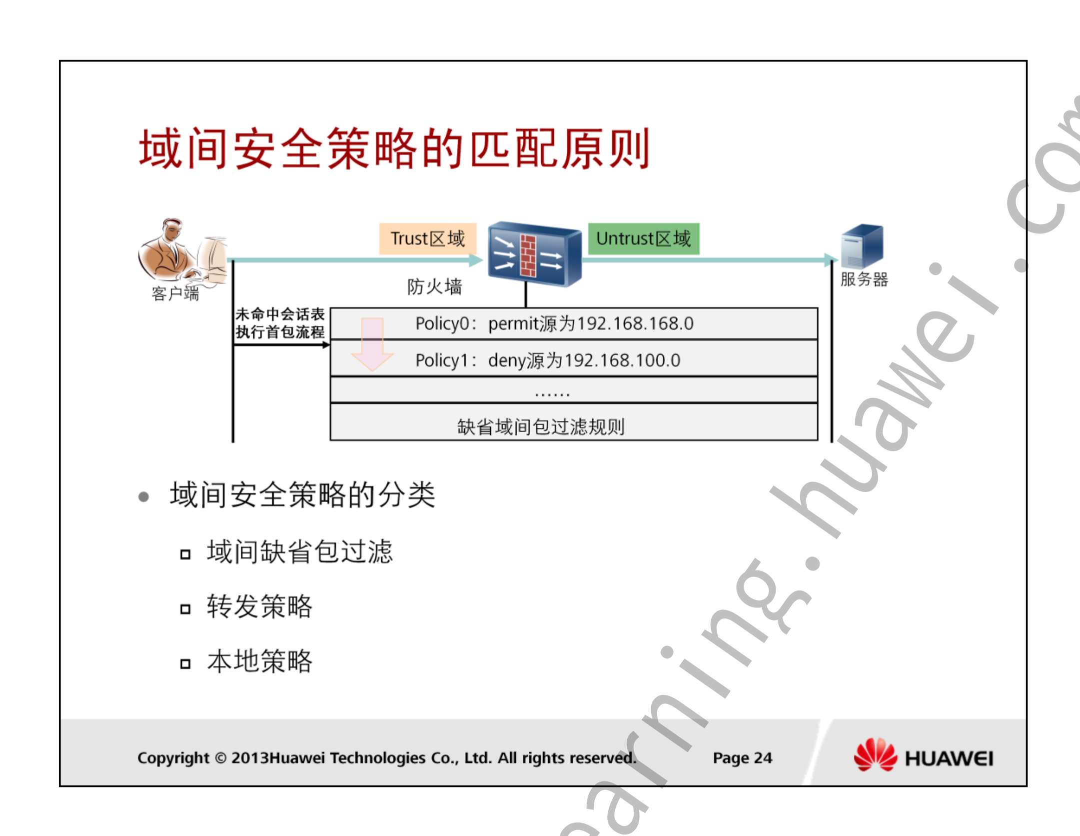
  Firewall interzone zone-name1 zone-name2

  lonk-link acl-number { inbound | outbound }

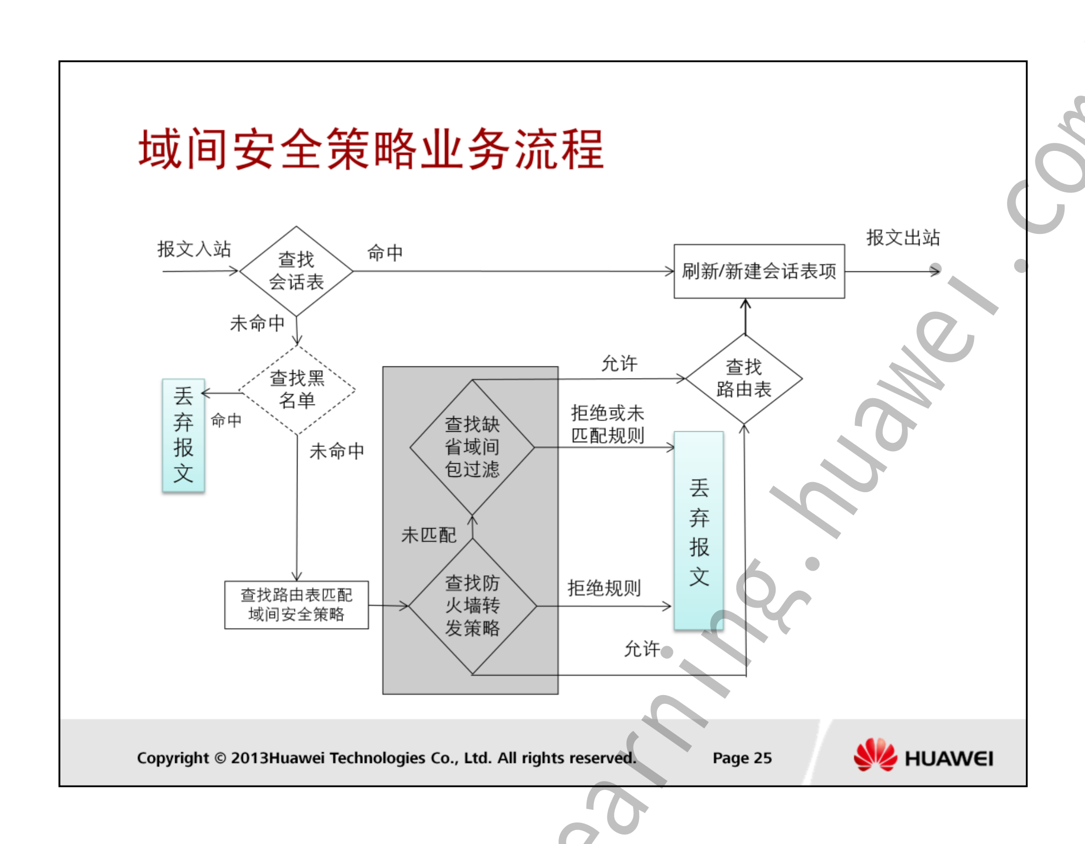


目录





- 域间缺省包过滤
  - 当数据流无法匹配域间安全策略时，会按照域间缺省包过滤规则来转发或丢弃该数据流的报文。
- 转发策略
  - 转发策略是指控制哪些流量可以经过设备转发的域间安全策略，对域间（除Local域外）转发流量进行安全检查，例如控制哪些Trust域的内网用户可以访问Untrust域的Internet。
- 本地策略
  - 本地策略是指与Local安全区域有关的域间安全策略，用于控制外界与设备本身的互访。



报文入站后，将首先匹配会话表，如果命中会话表，将进入后续包处理流程，刷新会话表时间，并直接根据会话表中的出接口，转发数据。

报文入站后，将首先匹配会话表，如果没有命中会话表，将进入首包包处理流程。依次进行黑名单检查，匹配域间安全策略，查找路由表，新建会话表，转发数据。

黑名单的实现原理就是：设备上建立一个黑名单表。对于接收到的报文的源IP地址存在于黑名单中，就将该报文予以丢弃。

黑名单分类：

- 静态黑名单

管理员可以通过命令行或Web方式手工逐个将IP地址添加到黑名单中。

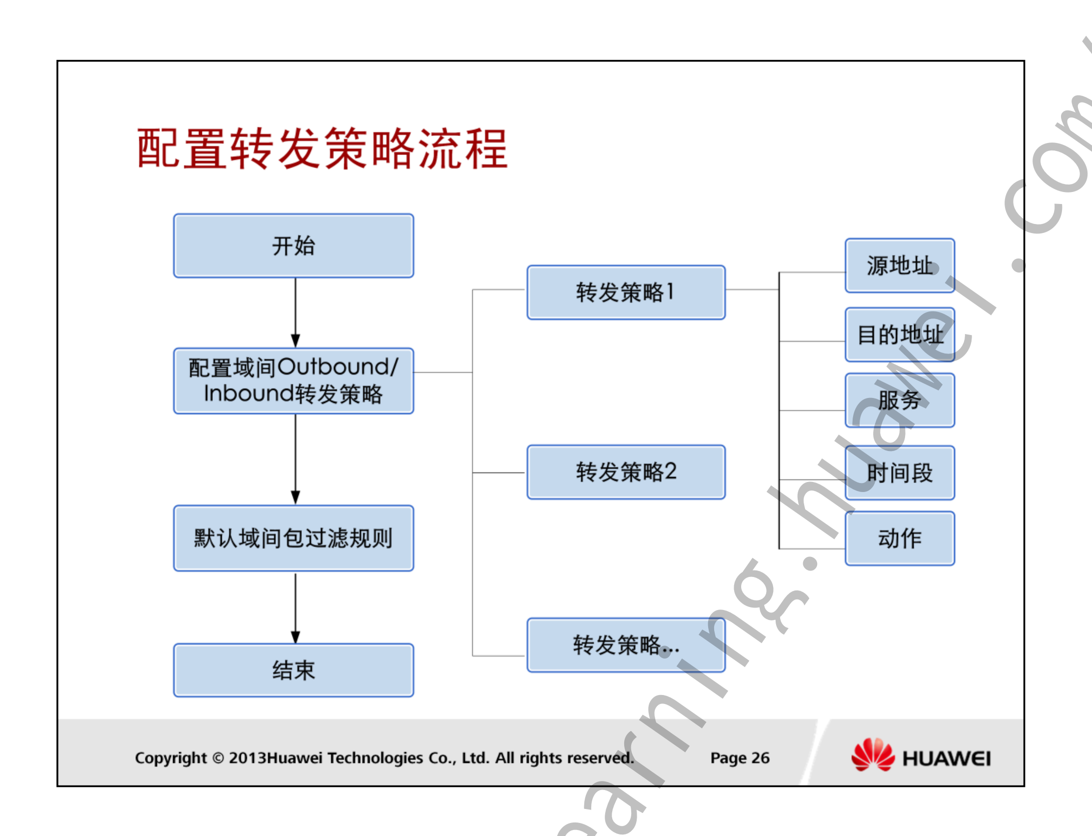
- 动态黑名单

转发策略和缺省域间包过滤优先级

转发策略优先于缺省域间包过滤匹配。设备将首先查找域间的转发策略，如果没有找到匹配项将匹配缺省包过滤进行处理。

- 刷新会话表

刷新会话表主要是刷新会话表老化时间，老化时间决定会话在没有相应的报文匹配的情况下，何时被系统删除。



- 转发策略的配置流程如图所示。
- 有两种思路来配置转发策略，根据需要选择。
  - 思路1：对安全性要求不高，开放缺省转发策略，然后只把个别需要拒绝的流量拒绝掉，出于安全性考虑不建议这种方式。
  - 思路2：关闭缺省转发策略，然后根据需要配置严格的转发策略。

配置转发策略（1）

- **进入域间安全策略视图**

  policy interzone *zone-name1 zone-name2* { inbound | outbound }

- 创建转发策略，并进入策略ID视图

  policy [*policy-id*]

- 指定需匹配流量的源地址（可选）

  policy source { *source-address* { *source-wildcard* | 0 | mask { *mask-address* | *mask-len* } } | address-set { *address-set-name* } &<1-256> | range *begin-address end-address* | any }

- 匹配流量的源地址的几种方法：（以源地址为例）

  policy source source-address source-wildcard

  policy source source-address 0

  policy source source-address mask { mask-address | mask-len }

  policy source address-set { address-set-name } &<1-256>

  policy source range begin-address end-address

  policy source source-address any

 Page 27



举例：

policy interzone trust untrust outbound

policy 0

action permit

policy source 192.168.168.0 0.255.0.255

policy service service-set http

同一个域间包过滤策略视图下可以为不同的流量创建不同的策略。缺省情况下，越先配置的策略，优先级越高，越先匹配报文。一旦匹配到一条Policy，就直接按照该Policy的定义处理报文，不再继续往下匹配。各个**policy**之间的优先级关系可以通过命令进行调整。

在包过滤策略视图下执行**policy** *policy-id* { **enable** | **disable** }，启用或者禁用一条自定义策略。

配置转发策略（1）

- 进入域间安全策略视图

  policy interzone *zone-name1 zone-name2* { inbound | outbound }

- 创建转发策略，并进入策略ID视图

  policy [*policy-id*]

- 指定需匹配流量的源地址（可选）

  policy source { *source-address* { *source-wildcard* | 0 | mask { *mask-address* | *mask-len* } } | address-set { *address-set-name* } &<1-256> | range *begin-address end-address* | any }

- 匹配流量的源地址的几种方法：（以源地址为例）

  policy source source-address source-wildcard

  policy source source-address 0

  policy source source-address mask { mask-address | mask-len }

  policy source address-set { address-set-name } &<1-256>

  policy source range begin-address end-address

  policy source source-address any



- source-wildcard点分十进制格式的通配符。
  - 例如：192.168.1.0 0.0.0.255，这里的0.0.0.255就是通配符。并且通配符的二进制形式支持1不连续，例如：0.255.0.255。 通配符转换为二进制后，为“0”的位是匹配值（源IP）中需要匹配的位，为“1”的位表示不需要关注。0.0.0.255的二进制形式是00000000 00000000 00000000 11111111，所以源IP地址是192.168.1.*的报文均能匹配到。
- 0通配符，表示主机。
- mask
  - mask-address 指定掩码。 点分十进制格式，形如255.255.255.0表示掩码长度为24。
  - mask mask-len 指定掩码长度。 整数形式，取值范围是1～32。
- address-set 指定地址集作为源IP地址。 可以指定1～256个地址集。
  - address-set-name 地址集名称。 字符串形式，不支持空格，支持除“-”、“?”和“,”以外的任意字符，长度范围是1～31个字符，不能以数字开头。
- range 指定源IP地址范围。 -
  - begin-address 起始IP地址。 点分十进制格式。
  - end-address 结束IP地址。 点分十进制格式。
- any 指定策略的源IP地址为任意IP地址。 -

如何使用反掩码

- 反掩码和子网掩码格式相似，但取值含义不同
  - 0表示对应的IP地址位需要比较
  - 1表示对应的IP地址位忽略比较
- 反掩码和IP地址结合使用，可以描述一个地址范围

怎样利用 IP 地址 和 反掩码wildcard-mask 来表示一个网段?

0	0	0	255	只比较前24位
0	0	3	255	只比较前22位
0	255	255	255	只比较前8位

 Page 29



举例：

192.168.10.0 0.0.0.255表示一个网段

192.168.10.1 0表示一个IP

思考：

在什么情况下，会使用0.255.0.255反掩码，其的作用和意义是什么？

此掩码表示对IP地址中A和C段进行掩码匹配，B和D段忽略。

配置转发策略（2）

- 指定需匹配流量的目的地址（可选）

  policy destination { *destination-address* { *destination-wildcard* | 0 | mask { *mask-address* | *mask-len* } } | address-set { *address-set-name* } &<1-256> | range *begin-address end-address* | any },

- 指定需匹配流量的服务集（可选）

  policy service service-set { *service-set-name* } &<1-256>

Address-set地址集

```
ip address-set  guest type object
address 0 192.168.12.0 0.0.0.15
address 1 192.168.15.0 0.0.0.63
address 2 192.168.30.0 0.0.0.127
```

Service-set服务集

```
ip service-set Internet type object
 service protocol tcp destination-port 80
 service protocol tcp destination-port 8080
 service protocol tcp destination-port 8443
```

 Page 30

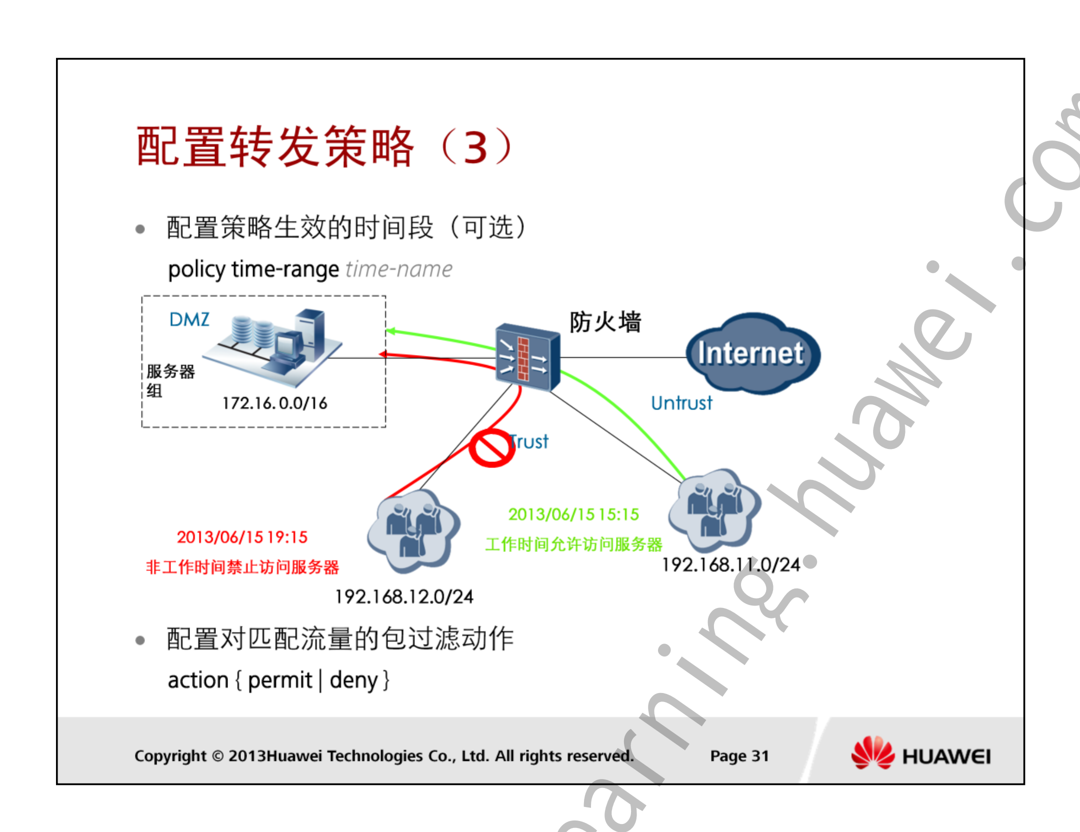


为简化配置和维护，防火墙支持引用地址集和服务集。除了提升配置和维护效率外，还使规则项更具可读性。

通过源/目的IP地址对流量进行控制时，可以将连续或不连续的地址加入地址集，然后在策略或规则中引用。

通过流量的服务类型（端口或协议类型）对流量进行控制时，可以使用预定义的知名服务集，也可以根据端口等信息创建自定义服务集，然后在策略或规则中引用。预定义服务集是系统缺省已经存在可以直接选择的服务类型。预定义服务通常都是知名协议，例如HTTP、FTP、Telnet等。自定义服务集是管理员通过指定端口号等信息来自行定义一些协议类型，也可以是各类服务集的组合。

地址集和服务集支持2种type，即object和group。type为group时，可以添加地址集或服务集作为成员。



如果需要对某一时间内发生的流量进行匹配和控制，可能通过使用基于时间段的访问控制列表。

在网络应用中，比较常见的应用是按照时间段开放某些网络应用，例如：上班时间不开放服务器某些端口，上班时间局域网的某些用户不能访问Internet等。这种特殊的应用前面所介绍的各种访问控制列表类型都无法满足要求，基于时间段访问控制列表可以精确的限定某个访问控制列表的生效时间，解决了访问控制列表在时间上一刀切的问题。

在定义时间段访问控制列表前，首先要在防火墙上定义一个时间段。

在包过滤策略视图下执行**policy** *policy-id* { **enable** | **disable** }，启用或者禁用一条自定义策略。

时间段配置

- **创建时间段**

time-range *time-name* { *start-time* **to** *end-time days* | **from** *time1 date1* [**to** *time2 date2*] }

操作符及语法	意义
HH:MM	From 某时间 To某时间
YYYY/MM/DD	From 某日期 To某日期
Mon/Tue/Wed/Thu/Fri/Sat/Sun	星期一/二/三/四/五/六/日
daily	一星期中的每天
off-day	休息日（星期六/日）
Working-day	工作日（星期一 至 星期五）



Time-range时间范围操作符，支持2种表现方式。一种是绝对时间段，即起止日期的时间段，另一种是周期时间段，即星期方式的时间段。

配置举例：

```
time-range work-policy1  08:00 to 18:00 working-day
time-range work-policy2  from 08:00 2013/01/01 to 18:00 2013/12/31
acl  2000
    rule permit ip source 192.168.11.0 0.0.0.255 time-range work-policy1
    rule permit ip source 192.168.12.0 0.0.0.255 time-range work-policy2
policy interzone trust untrust outbound
    policy 1
    Policy source 192.168.11.0 0.0.0.255
    policy time-range work-policy1
    policy 2
    Policy source 192.168.12.0 0.0.0.255
    policy time-range work-policy2
```



在Web配置界面下，配置转发策略的步骤为：

1. 选择“防火墙 > 安全策略 > 转发策略”。
2. 在“转发策略列表”中，单击“新建”。
3. 依次输入或选择各项参数。
4. 单击“应用”。

配置本地策略（命令行）

- 进入域间安全策略视图

  policy interzone local *zone-name* { inbound | outbound }

- 创建转发策略，并进入策略ID视图

  policy [*policy-id*]

- 指定需匹配流量的源地址（可选）

  policy source { *source-address* { *source-wildcard* | **0** | **mask** { *mask-address* | *mask-len* } } | **address-set** { *address-set-name* } &<1-256> | **range** *begin-address end-address* | **any** }

- 指定需匹配流量的目的地址（可选）

  policy destination { *destination-address* { *destination-wildcard* | **0** | **mask** { *mask-address* | *mask-len* } } | **address-set** { *address-set-name* } &<1-256> | **range** *begin-address end-address* | **any** }，

- 指定需匹配流量的服务集（可选）

  policy service service-set { *service-set-name* } &<1-256>，

- 配置对匹配流量的包过滤动作

  action { **permit** | **deny** }



举例：

policy interzone trust local inbound

policy 0

action permit

policy source 10.1.1.1 0

policy service service-set telnet

在域间安全策略视图下执行policy policy-id { enable | disable }，启用或者禁用一条策略。



在Web配置界面下，配置本地策略的步骤为：

1. 选择“防火墙 > 安全策略 > 本地策略”。
2. 在“对设备访问控制列表”中，单击“新建”。
3. 依次输入或选择各项参数。
4. 单击“应用”。

配置域间缺省包过滤（命令行）

- 配置防火墙内部的所有域间缺省包过滤

  firewall packet-filter default { *permit* | *deny* } **all** [direction { *inbound* | *outbound* }]

  举例：所有域间缺省包过滤规则为Permit

  firewall packet-filter default permit all

- 配置根防火墙或虚拟防火墙内部的某个域间缺省包过滤

  firewall packet-filter default { *permit* | *deny* } **interzone** *zone-name1 zone-name2* **[direction { inbound | outbound }]**

  举例：源Trust->目的Untrust域间缺省包过滤规则为**Permit**

  firewall packet-filter default permit interzone Trust Untrust direction outbound

- 查看当前域间配置的缺省包过滤规则

  display firewall packet-filter default all查看所有域间的配置

  或者display firewall packet-filter default interzone zone-name1 zone-name2查看某个域间的配置

  。

Page 36



USG2200/5100/5500缺省出厂配置:

- 允许通过:
  - Local域到其他任意安全区域Outbound方向的报文
  - Trust域到Local域的Outbound和Inbound报文；
- 禁止通过：
  - 其他安全区域间的所有方向都禁止报文通过。

USG2200/USG5100 BSR/HSR缺省出厂配置：

- 允许通过:
  - 所有安全区域间的所有方向的报文

配置域间缺省包过滤（Web方式）

- 当数据流无法匹配域间安全策略时，会按照域间缺省包过滤规则来转发或丢弃该数据流的报文。

防火墙 > 安全策略 > 转发策略

修改转发策略

源安全区域	untrust
目的安全区域	trust
源地址	any
目的地址	any
用户	请选择或输入用户或用户组
服务	请选择服务
时间段	all
动作	deny

应用 返回

 Page 37 HUAWEI

可以通过以下命令配置域间缺省包过滤

firewall packet-filter default { permit | deny } all [direction { inbound | outbound }]

根据对安全性的要求进行配置，如果开启缺省包过滤会造成没有匹配具体安全策略的数据流都允许通过设备。一般情况下建议保持关闭，然后配置具体允许哪些数据流通过的安全策略。

配置域内安全策略

- 进入域内安全策略视图

  policy zone *zone-name*

- 创建域内安全策略，并进入策略ID视图

  policy [*policy-id*]

- 指定需匹配流量的源地址（可选）

  policy source { *source-address* { *source-wildcard* | **0** | **mask** { *mask-address* | *mask-len* } } | **address-set** { *address-set-name* } &<1-256> | **range** *begin-address end-address* | **any** }

- 指定需匹配流量的目的地址（可选）

  policy destination { *destination-address* { *destination-wildcard* | **0** | **mask** { *mask-address* | *mask-len* } } | **address-set** { *address-set-name* } &<1-256> | **range** *begin-address end-address* | **any** }，

- 指定需匹配流量的服务集（可选）

  policy service service-set { *service-set-name* } &<1-256>，

- 配置对匹配流量的包过滤动作

  action { **permit** | **deny** }



举例：

policy zone trust

policy 0

action deny

policy service service-set ftp

policy source 1.1.1.1 0

policy destination 10.1.1.1 0

在域内安全策略视图下执行policy policy-id { enable | disable }，启用或者禁用一条策略。

配置接口包过滤

- 进入接口视图

  interface *interface-type interface-number*

- 在接口上的一个方向上应用一条基本或高级ACL规则

  firewall packet-filter *acl-number* { **inbound** | **outbound** }

- 应用一条基于MAC地址的ACL

  firewall ethernet-frame-filter *acl-number* inbound

- 应用一条硬件包过滤的ACL

  hardware-filter *acl-number* inbound

 Page 39 

在基于基本或高级ACL的接口包过滤中，inbound指接口收到的报文，outbound指接口发送的报文。在基于MAC地址的包过滤中，只支持inbound一个方向，即只对接口收到的报文进行过滤。在硬件包过滤中，只支持inbound一个方向，即只对接口收到的报文进行过滤。

每个接口只能应用一条ACL。如果重复配置，新配置的ACL将覆盖旧的ACL。

- ACL定义的数据流有很大区别：
  - 基本ACL2000～2999仅使用源地址信息进行流量匹配。
  - 高级ACL3000～3999可以使用数据包的源地址、目的地址、IP承载的协议类型、源端口、目的端口等5元组信息进行流量匹配。
  - 基于MAC地址ACL4000～4999主要用于对以太网等数据链路层协议帧头中的源MAC地址、目的MAC地址、类型字段等信息进行流量匹配。
  - 硬件包过滤ACL是一种特殊的ACL，将硬件包过滤ACL下发到接口卡上后，接口卡通过硬件实现包过滤功能，比普通的软件包过滤速度更快，消耗系统资源更少。硬件包过滤ACL的匹配条件比较全面，可以通过源IP地址、目的IP地址、源MAC地址、目的MAC地址、协议等维度来进行流量匹配。

配置接口包过滤

- 进入接口视图

  interface *interface-type interface-number*

- 在接口上的一个方向上应用一条基本或高级ACL规则

  firewall packet-filter *acl-number* { **inbound** | **outbound** }

- 应用一条基于MAC地址的ACL

  firewall ethernet-frame-filter *acl-number* inbound

- 应用一条硬件包过滤的ACL

  hardware-filter *acl-number* inbound

 Page 40



- 创建高级ACL， 并进入ACL视图

  acl [**number**] *acl-number* [**vpn-instance** *vpn-instance-name*] [**match-order** { **config** | **auto** }]

- 配置指定协议信息的高级ACL规则

  举例：rule deny tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port equal www

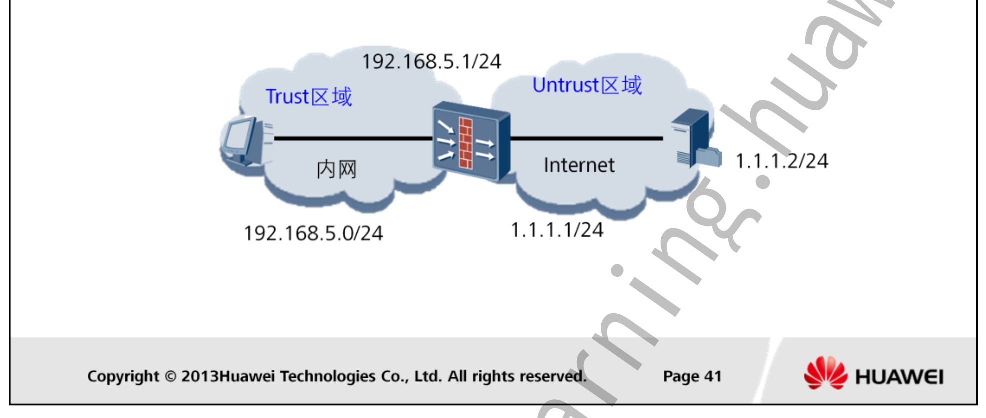
- 查看ACL匹配情况

  <USG5000>display ACL 2001

  rule 0 permit source 10.32.255.0 0.0.0.255 （27 times matched）

  从例子中可以看出ACL 2001中规则的匹配情况，给故障诊断提供了依据，具体步骤参考故障诊断。

- ACL的应用场景
  - 防火墙接口包过滤应用
  - QoS应用
  - 策略路由应用
  - 路由策略应用
  - IPSec应用



配置思路：

1. 规划转发策略。

需求是需要允许192.168.5.0/24这个大范围的网段通过，然后拒绝这个范围内的几个特殊IP。这样需要配置2条转发策略，先配置拒绝特殊IP通过的转发策略，然后再配置允许整个网段通过的转发策略。如果配置反了，几个特殊的IP就会先匹配上大范围的策略通过防火墙了，不会再继续匹配下边的特殊策略了。

2. 地址集规划。

需求中是通过IP地址控制访问权限，那么需要在转发策略中指定IP地址作为匹配条件。对于连续的地址段可以在策略中直接配置，但是对于零散的地址建议配置为地址集，对地址集进行统一控制，而且也方便被其他策略复用。所以在本例中可以将几个特殊的IP地址配置成一个地址集。

3. 配置转发策略，控制上网权限。

关键配置（命令行）

- 创建拒绝特殊的几个IP地址访问Internet的转发策略

[USG] policy interzone trust untrust outbound

[USG-policy-interzone-trust-untrust-outbound] policy 0

[USG-policy-interzone-trust-untrust-outbound-0] policy source address-set ip_deny

[USG-policy-interzone-trust-untrust-outbound-0] action deny

- 创建允许192.168.5.0/24这个网段访问Internet的转发策略

[USG-policy-interzone-trust-untrust-outbound] policy 1

[USG-policy-interzone-trust-untrust-outbound-1] policy source 192.168.5.0 mask 24

[USG-policy-interzone-trust-untrust-outbound-1] action permit

 Page 42



ip_deny地址集配置如下：

[USG] ip address-set ip_deny type object

[USG-object-address-set-ip_deny] address 192.168.5.2 0

[USG-object-address-set-ip_deny] address 192.168.5.3 0

[USG-object-address-set-ip_deny] address 192.168.5.6 0

关键配置1（Web）

- 配置名称为ip_deny的地址组

防火墙 > 地址 > 地址组

新建地址组

名称 ip_deny *

描述

引用地址或地址组 可选 已选

全选 清空

配置IP地址 新建 删除

子网/IP范围	描述
192.168.5.2/32	
192.168.5.3/32	
192.168.5.6/32	

应用 返回

Page 43 HUAWEI

配置名称为deny_ip的地址组，将几个不允许上网的IP地址加入地址组。

1. 选择“防火墙 > 地址 > 地址组”。
2. 在“地址组列表”中单击，进入“新建地址组”界面。
3. 配置地址组的名称和描述信息。

关键配置2（Web）

- 配置拒绝特殊地址组ip_deny内IP地址访问Internet的转发策略







防火墙转发策略配置步骤：

1. 选择"防火墙 > 安全策略 > 转发策略"。
2. 选择"转发策略"页签。
3. 在"转发策略列表"中单击 新建 。
4. 输入或选择相应参数。
5. 单击"应用"



总结

- 防火墙包过滤技术原理
- 防火墙转发原理
- 防火墙安全策略应用场景及配置方法



思考题

- 包过滤与状态检测机制、会话表之间有哪些关联关系?
- Server Map表项的具体的作用是什么?
- 分片缓存中首报分片和其它分片在报文格式上有何区别？首包分片先到如何处理？首包分片晚到如何处理?
- 端口识别（端口映射）主要应用于什么场景下?
- 域间安全策略Inbound和Outbound有何区别?



Thank you

www.huawei.com

HC110310004

HCNA-Security-CBSN 第四章 网络地址转换技术


第四章
网络地址转换技术
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目标

- 学完本课程后，您将能够:
  - 掌握NAT的技术原理
  - 掌握NAT几种应用方式
  - 掌握防火墙的NAT配置





目录



NAT产生背景

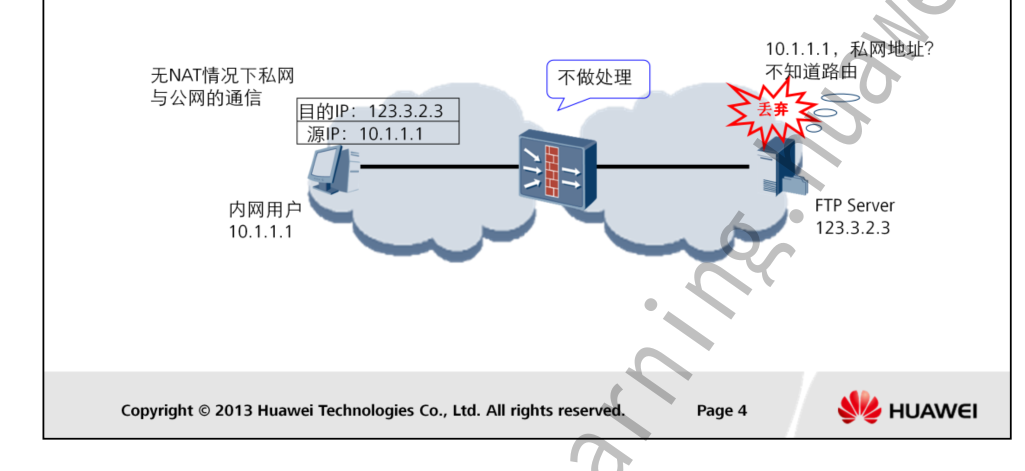
- IPv4地址日渐枯竭
- IPv6技术不能立即大面积替换
- 各种延长IPv4寿命的技术不断出现，NAT就是其中之一。

Page 3
HUAWEI

早在上世纪90年代初，有关RFC文档就提出IP地址耗尽的可能性。基于TCP/IP协议的Web应用使互联网迅速扩张，IPv4地址申请量越来越大。互联网可持续发展的问题日益严重。中国的运营商每年向ICANN申请的IP地址数量为全球最多。曾经有专家预言，根据互联网的发展速度，到2011年左右，全球可用的IPv4地址资源将全部耗尽。

IPv6的提出，就是为了从根本上解决IPv4地址不够用的问题。IPv6地址集将地址位数从IPv4的32位扩展到了128位。对于网络应用来说，这样的地址空间几乎是无限大。因此IPv6技术可以从根本上解决地址短缺的问题。但是，IPv6面临着技术不成熟、更新代价巨大等尖锐问题，要想替换现有成熟且广泛应用的IPv4网络，还有很长一段路要走。

既然不能立即过渡到IPv6网络，那么必须使用一些技术手段来延长IPv4的寿命。而技术的发展确实有效延缓了IPv4地址的衰竭，专家预言的地址耗尽的情况并未出现。其中广泛使用的技术包括无类域间路由（CIDR， Classless Inter-Domain Routing）、可变长子网掩码（VLSM， Variable Length Subnet Mask）和网络地址转换（NAT， Network Address Translation）。



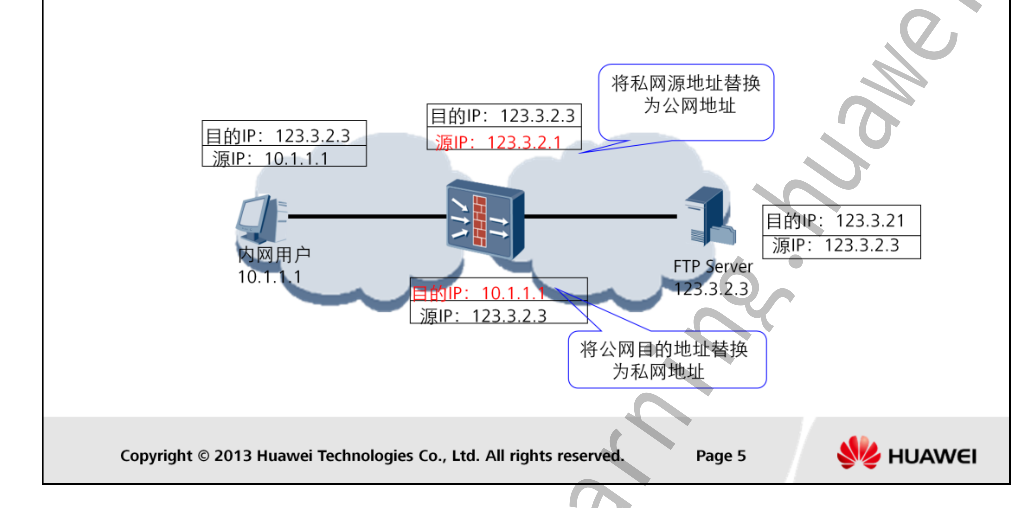
私网地址出现的目的是为了实现地址的复用，提高IP地址资源的利用率，为了满足一些实验室、公司或其他组织的独立于Internet之外的私有网络的需求，RFCA（Requests For Comment）1918为私有使用留出了三个IP地址段。具体如下：

- A类IP地址中的10.0.0.0～10.255.255.255（10.0.0.0/8）
- B类IP地址中的172.16.0.0～172.31.255.255（172.16.0.0/12）
- C类IP地址中的192.168.0.0～192.168.255.255（192.168.0.0/16）

上述三个范围内的地址不能在Internet上被分配，因而可以不必申请就可以自由使用

内网使用私网地址，外网使用公网地址，如果没有NAT将私网地址转换为公网地址，会造成通信混乱，最直接的后果就是无法通信。

使用私网地址和外网进行通信，必须使用NAT技术进行地址转换，保证通信正常。



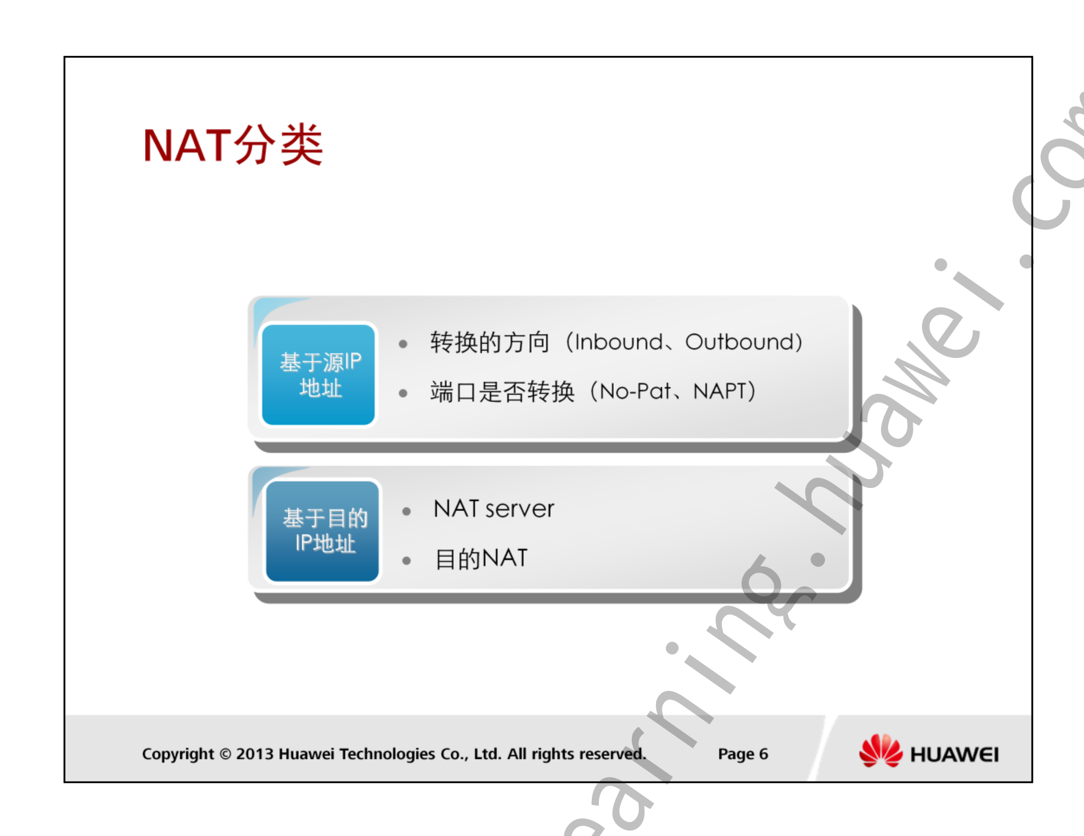
NAT是将IP数据报文报头中的IP地址转换为另一个IP地址的过程，主要用于实现内部网络（私有IP地址）访问外部网络（公有IP地址）的功能。从实现上来说，一般的NAT转换设备（实现NAT功能的网络设备）都维护着一张地址转换表，所有经过NAT转换设备并且需要进行地址转换的报文，都会通过这个表做相应的修改。

地址转换的机制分为如下两个部分：

- 内部网络主机的IP地址和端口转换为NAT转换设备外部网络地址和端口。
- 外部网络地址和端口转换为NAT转换设备内部网络主机的IP地址和端口。

也就是<私有地址+端口>与<公有地址+端口>之间相互转换。

NAT转换设备处于内部网络和外部网络的连接处。内部的PC与外部服务器的交互报文全部通过该NAT转换设备。常见的NAT转换设备有路由器、防火墙等。



NAT功能包括对源IP地址进行转换，和对目的IP地址进行转换两种方式。

其中，基于源IP地址的转换可以从以下两个方面进行划分：

- 转换的方向。按照转换的方向可以将源IP地址转换划分为以下两类：
  - Inbound方向：数据包由低安全级别的安全区域向高安全级别的安全区域方向传输时，基于源IP地址进行的转换。
  - Outbound方向：数据包由高安全级别的安全区域向低安全级别的安全区域方向传输时，基于源IP地址进行的转换。
- 端口是否转换。按照端口是否转换可以将源IP地址转换划分为以下两类：
  - No-PAT(Port Address Translation)方式的NAT：主要用于一对一的IP地址的转换，端口不进行转换。
  - NAPT(Network Address Port Translation)方式的NAT：主要用于多对一或多对多的地址转换，转换时地址和端口号同时进行转换。

按照功能不同，可以将基于目的IP地址的转换分为以下两类：

- NAT Server：主要应用于实现私网服务器以公网IP地址对外提供服务的场景。
- 目的NAT：主要应用于实现手机用户上网时，手机的缺省WAP网关与所在地运营商的实际WAP网关不一致，导致需要修改报文的目的网关地址的场景。

NAT分类

- 基于源IP地址
  - 转换的方向（Inbound、Outbound）
  - 端口是否转换（No-Pat、NAPT）
- 基于目的IP地址
  - NAT server
  - 目的NAT

 Page 7 HUAWEI

在某些场景下，既要对源IP地址进行转换，又要对目的IP地址进行转换，被称为双向NAT。常见的场景包括：

- NAT Inbound和NAT Server一起使用：主要用于简化配置NAT Server时的路由配置。
- 域内NAT和NAT Server一起使用：主要应用于实现私网用户以公网地址访问属于同一安全区域的私网服务器的场景。

NAT的优点与缺点

- 优点
  - 实现IP地址复用，节约宝贵的地址资源
  - 地址转换过程对用户透明
  - 对内网用户提供隐私保护
  - 可实现对内部服务器的负载均衡
- 缺点
  - 网络监控难度加大
  - 限制某些具体应用

 Page 8



NAT技术除了可以实现地址复用，节约宝贵IP地址资源的优点外，还有其他一些优点，NAT技术的发展，也不断吸收先进的理念，总的来说，NAT的优点和不足如下：

- NAT的优点

可以使一个局域网中的多台主机使用少数的合法地址访问外部的资源，也可以设定内部的WWW、FTP、Telnet等服务提供给外部网络使用，解决了IP地址日益短缺的问题。

对于内外网络用户，感觉不到IP地址转换的过程，整个过程对于用户来说是透明的。

对内网用户提供隐私保护，外网用户不能直接获得内网用户的IP地址、服务等信息，具有一定的安全性。

通过配置多个相同的内部服务器的方式可以减小单个服务器在大流量时承担的压力，实现服务器负载均衡。

- NAT的不足

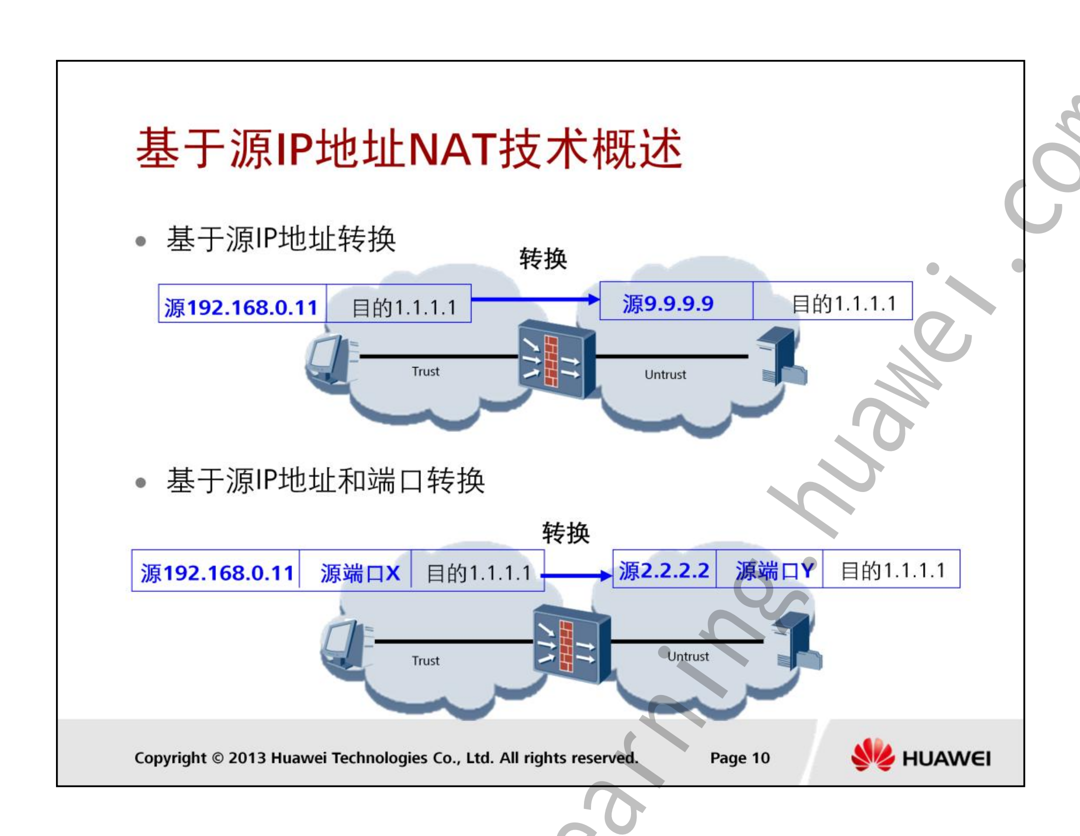
由于需要对数据报文进行IP地址的转换，涉及IP地址的数据报文的报头不能被加密。在应用协议中，如果报文中有地址或端口需要转换，则报文不能被加密。例如，不能使用加密的FTP连接，否则FTP的port命令不能被正确转换。

网络监管变得更加困难。例如，如果一个黑客从内网攻击公网上的一台服务器，那么要想追踪这个攻击者很难。因为在报文经过NAT转换设备的时候，地址经过了转换，不能确定哪台才是黑客的主机。



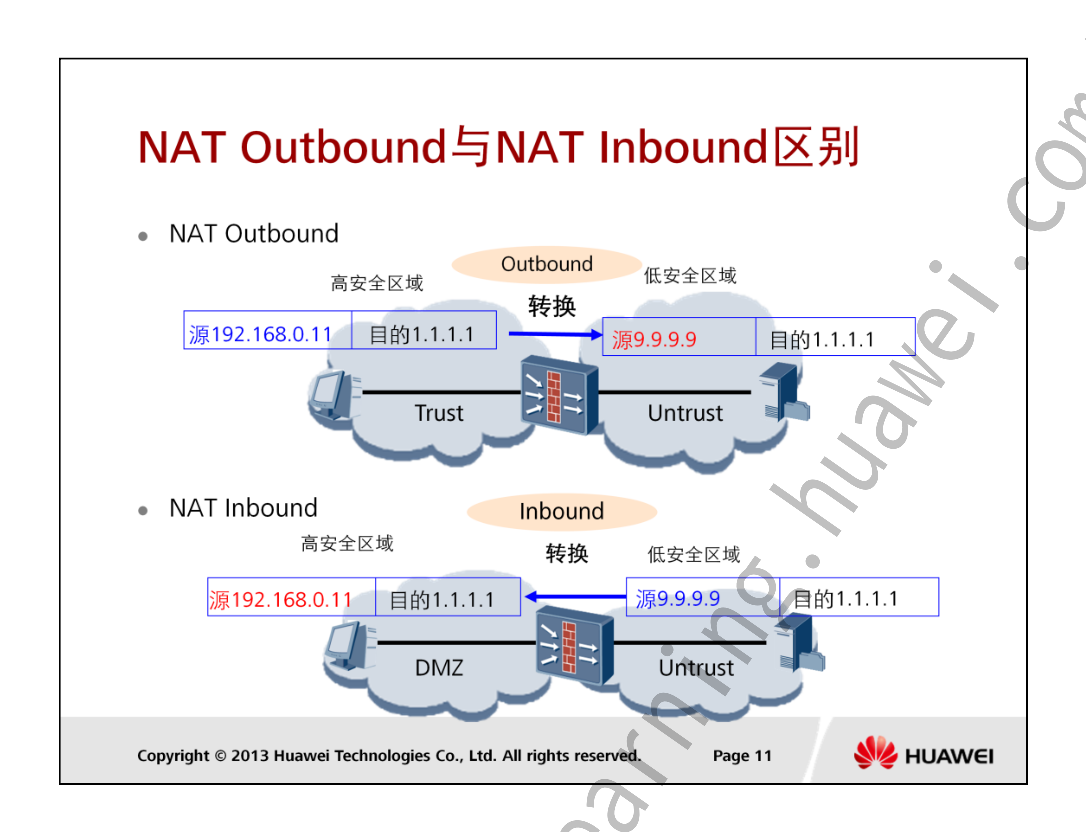
目录





基于源IP地址的NAT是指对发起连接的IP报文头中的源地址进行转换。它可以实现内部用户访问外部网络的目的。通过将内部主机的私有地址转换为公有地址，使一个局域网中的多台主机使用少数的合法地址访问外部资源，有效的隐藏了内部局域网的主机IP地址，起到了安全保护的作用。由于一般内网区域的安全级别比外网高，所以这种应用又称为NAT Outbound。

基于源IP地址和端口转换，一般情况下源端口X=源端口Y，即保持原端口信息，并表现在会话表项。此种转化方式需保证会话表项的唯一性。



NAT Outbound与NAT Inbound区别，主要在于基于源IP地址转换是由高优先级至低优先级，还是低优先级至高优先级。他们的共同点都是进行源IP地址转换。

基于端口是否转换的NAT

- No-PAT(Port Address Translation)。主要用于一对一的IP地址的转换，端口不进行转换。

192.168.1.1	→	155.133.87.1
192.168.1.2	→	155.133.87.2
192.168.1.3	→	155.133.87.3
192.168.1.4	→	丢弃

- 将不同的内部地址映射到同一公有地址的不同端口号上，实现多对一地址转换。主要利用NAPT技术实现多对一地址转换。

192.168.1.1	→	155.133.87.1：7111
192.168.1.2	→	155.133.87.1：7112
192.168.1.3	→	155.133.87.1：7113

 Page 12



NAT No-PAT可以称为“一对一地址转换”，在地址转换过程中，数据包的源IP地址由私网地址转换为公网地址，但端口号不做转换。

例如，地址池中的公网IP地址只有两个。由于一台私网主机在借用其中的一个公网IP访问公网时，会占用这个IP的所有端口。因此，这种情况只允许最多有两台私网主机同时访问公网，其他的私网主机要等到其中一台主机不再访问公网，它占用的公网IP地址被释放后，才可以再进行NAT访问公网。

网络地址端口转换（NAPT， Network Address Port Translation）也能实现并发的地址转换。它允许多个内部地址使用一个公有地址访问Internet，也可称之为“多对一地址转换”或 “地址复用”。

NAPT是一种利用第四层信息来扩展第三层地址的技术，一个IP地址有65535个端口可以使用。理论上来说，一个地址可以为其他65535个地址提供NAPT转换，NAPT还能将来自不同内部地址的数据报文映射到同一公有地址的不同端口号上，因而仍然能够共享同一地址，对比一对一或多对多地址转换。这样极大的提升了地址空间，增加了IP地址的利用率。 因此NAPT是最常用的一种地址转换方式。

在NAPT方式中，还可以直接借用设备与外网相连的接口的IP地址作为转换后的IP地址，这种借用接口IP做NAT的应用又称为easy-ip。直接借用接口IP地址作为公网地址的情况下，不需要创建NAT地址池。

基于源IP地址转换的配置（命令行）

- 在系统视图下，配置NAT地址池

  nat address-group group-number [group-name] start-address end-address

- 在系统视图下，进入域间NAT策略视图

  nat-policy interzone zone-name1 zone-name2 {inbound | outbound}

- 创建NAT策略，进入策略ID视图

  policy [policy-id]

  Policy source { source-address source-wildcard |......}

  Policy destination { source-address source-wildcard |......}

  Policy service service-set {service-set-name}

  action { source-nat |no-nat}

  Address-group {number | name} **no-pat**

 Page 13



NAT地址池是指用NAT转换时用于分配的公网IP地址范围。进行转换时，设备会从该地址池中随机选择一个地址，用于替换报文中的源IP地址。不进行端口转换。

进入NAT域间进行NAT转换的源IP地址所在的两个安全区域，域间的方向的选择与包过滤一致，当源地址所在安全区域的优先级比目的地址所在安全区域高，则应选择outbound，反之，则应选择inbound。在NAT No-pat应用中，需要进行NAT转换的源IP地址是内网用户的IP地址，所以此处的流的方向应该是从内网流入外网。外网安全区域的安全级别一般比内网低，所以这里一般选择outbound。

同一个域间NAT策略视图下可配置多个NAT策略。缺省情况下，越先配置的策略，优先级越高，越先匹配报文。

NAPT与NAT No-pat主要区别在于，NAPT除了转换源IP地址外，还进行端口转换，即不需要配置no-pat参数。

在NAPT情况下，若直接使用设备与外网相连的接口的IP地址作为转换后的源IP地址，可执行命令**easy-ip** *interface-type interface-number*，配置NAT策略直接引用接口IP地址。

NAT 地址池

- NAT地址池是一些连续的IP地址集合，当来自私网的报文通过地址转换到公网IP时，将会选择地址池中的某个地址作为转换后的地址
  - 创建NAT地址池的命令为：

    nat address-group *group-number* [*group-name*] *start-address end-address* [vrrp *virtual-router-ID*]

  - nat address-group 0 pool0 192.168.1.1 192.168.1.100



 Page 14



NAT地址池中的地址可以是一个公网IP地址，也可以是多个公网IP地址。

在配置基于源IP地址的NAT与域内NAT时，需要首先配置NAT地址池，然后将NAT地址池与policy绑定，通过选择不同的参数，实现不同功能的NAT。

在配置NAT地址池的时候，地址池中的地址个数不能超过4096。当地址个数超过256时，该地址池只能被No-PAT的方式引用。

当某地址池已经和policy关联时，不允许删除这个地址池。

配置NAT地址池时，应将上网接口地址和地址池配置在同一网段，即和分配的公网IP地址在同一网段；如果地址池所在网段与上网接口不在同一个网段，注意需要在USG的下一跳路由器上配置到地址池的路由。

当设备同时应用于双机热备组网时，如果NAT地址池地址与VRRP备份组虚拟IP地址不在同一网段，不需要配置vrrp关键字；如果NAT地址池中的地址与VRRP备份组虚拟IP地址在同一网段，需要配置vrrp关键字，且*virtual-router-id*为NAT出接口对应的VRRP备份组的ID。否则可能导致业务中断。



在Web配置界面中，配置NAT地址池的步骤为：

1. 选择“防火墙 > NAT > 源NAT > NAT地址池”。
2. 在“NAT地址池列表”中，单击“新建”。
3. 依次输入或选择各项参数。

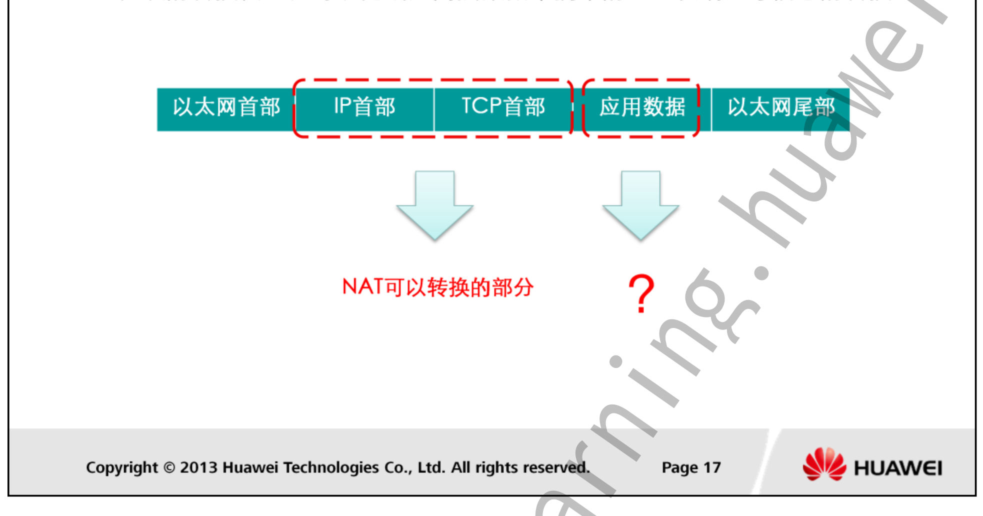


基于源IP地址转换的配置步骤为：

1. 选择“防火墙 > NAT > 源NAT > 源NAT”。
2. 在“源NAT策略列表”中，单击“新建”。
3. 依次输入或选择各项参数。

在使用Web配置界面中，没有单独设置outbound和inbound的选项，对于inbound和outbound方向的指定，根据源安全区域和目的安全区域来确定。

如果设置转换后的IP地址为接口IP地址，则该种方式等同于命令行中的esay ip命令。



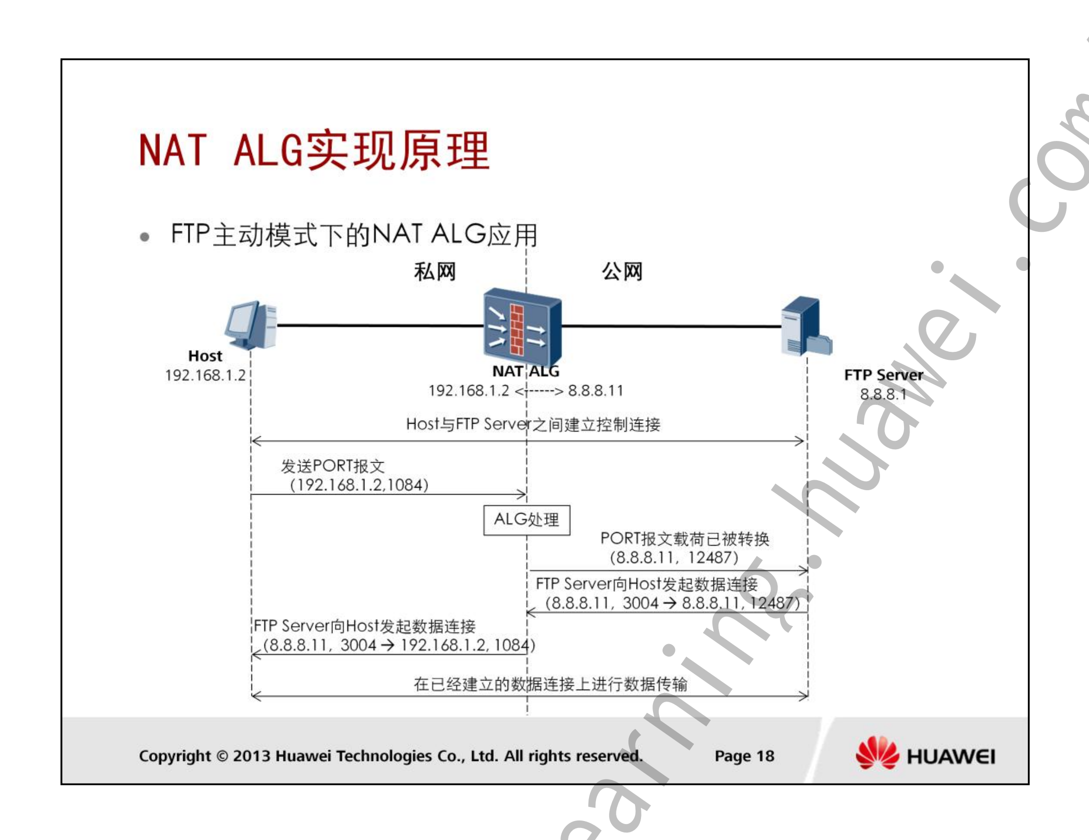
在以太网数据帧结构中，IP首部包含32位的源IP地址和32位的目的IP地址，TCP首部包含16位的源端口号和16位的目的端口号。

但是很多协议会通过IP报文的数据载荷进行新端口甚至新IP地址的协商。协商完成之后，通信双方会根据协商结果建立新的连接进行后续报文的传输。而这些协商出来的端口和IP地址往往是随机的，管理员并不能为其提前配置好相应的NAT规则，这些协议在NAT转换过程中就会出现问题。

普通NAT实现了对UDP或TCP报文头中的的IP地址及端口转换功能，但对应用层数据载荷中的字段无能为力，在许多应用层协议中，比如多媒体协议（H.323、SIP等）、FTP、SQLNET等，TCP/UDP载荷中带有地址或者端口信息，这些内容不能被NAT进行有效的转换，就可能导致问题。而NAT ALG（Application Level Gateway，应用层网关）技术能对多通道协议进行应用层报文信息的解析和地址转换，将载荷中需要进行地址转换的IP地址和端口或者需特殊处理的字段进行相应的转换和处理，从而保证应用层通信的正确性。

例如，FTP应用就由数据连接和控制连接共同完成，而且数据连接的建立动态地由控制连接中的载荷字段信息决定，这就需要ALG来完成载荷字段信息的转换，以保证后续数据连接的正确建立。

为了实现应用层协议的转发策略而提出了ASPF功能。ASPF功能的主要目的是通过对应用层协议的报文分析，为其开放相应的包过滤规则，而NAT ALG的主要目的，是为其开放相应的NAT规则。由于两者通常都是结合使用的，所以使用同一条命令就可以将两者同时开启。



图中私网侧的主机要访问公网的FTP服务器。NAT设备上配置了私网地址192.168.1.2到公网地址8.8.8.11的映射，实现地址的NAT转换，以支持私网主机对公网的访问。组网中，若没有ALG对报文载荷的处理，私网主机发送的PORT报文到达服务器端后，服务器无法根据私网地址进行寻址，也就无法建立正确的数据连接。整个通信过程包括如下四个阶段：

1. 私网主机和公网FTP服务器之间通过TCP三次握手成功建立控制连接。
2. 控制连接建立后，私网主机向FTP服务器发送PORT报文，报文中携带私网主机指定的数据连接的目的地址和端口，用于通知服务器使用该地址和端口和自己进行数据连接。
3. PORT报文在经过支持ALG特性的NAT设备时，报文载荷中的私网地址和端口会被转换成对应的公网地址和端口。即设备将收到的PORT报文载荷中的私网地址192.168.1.2转换成公网地址8.8.8.11，端口1084转换成12487。
4. 公网的FTP服务器收到PORT报文后，解析其内容，并向私网主机发起数据连接，该数据连接的目的地址为8.8.8.11，目的端口为12487（注意：一般情况下，该报文源端口为20，但由于FTP协议没有严格规定，有的服务器发出的数据连接源端口为大于1024的随机端口，如本例采用的是wftpd服务器，采用的源端口为3004）。由于该目的地址是一个公网地址，因此后续的数据连接就能够成功建立，从而实现私网主机对公网服务器的访问。

NAT与Server Map表

- NAT ALG通过 server-map表中的转换字段，可以转换上层的信息
- NAT中生成Server-map表项 的两种情况：

配置NAT Server	配置NAT No-PAT
设备会自动生成Server-map表项，用于存放Global地址与Inside地址的映射关系。	设备会为已配置的多通道协议产生的有实际流量的数据流建立Server-map表。



通常情况下，如果在设备上配置严格包过滤，那么设备将只允许内网用户单方向主动访问外网。但在实际应用中，例如使用FTP协议的port方式传输文件时，既需要客户端主动向服务器端发起控制连接，又需要服务器端主动向客户端发起服务器数据连接，如果设备上配置的包过滤为允许单方向上报文主动通过，则FTP文件传输不能成功。

为了解决这一类问题，USG设备引入了Server-map表，Server-map用于存放一种映射关系，这种映射关系可以是控制数据协商出来的数据连接关系，也可以是配置NAT中的地址映射关系，使得外部网络能透过设备主动访问内部网络。

生成Server-map表之后，如果一个数据连接匹配了Server-map表项，那么就能够被设备正常转发，而不需要去查会话表，这样就保证了某些特殊应用的正常转发。

- 配置NAT Server成功后，设备会自动生成Server-map表项，用于存放Global地址与Inside地址的映射关系。

  当不配置“no-reverse”参数时，每个生效的NAT Server都会生成正反方向两个静态的Server-map；当配置了“no-reverse”参数时，生效的NAT Server只会生成正方向静态的Server-map。用户删除NAT Server时，Server-map也同步被删除。

- 配置NAT No-PAT后，设备会为已配置的多通道协议产生的有实际流量的数据流建立Server-map表。

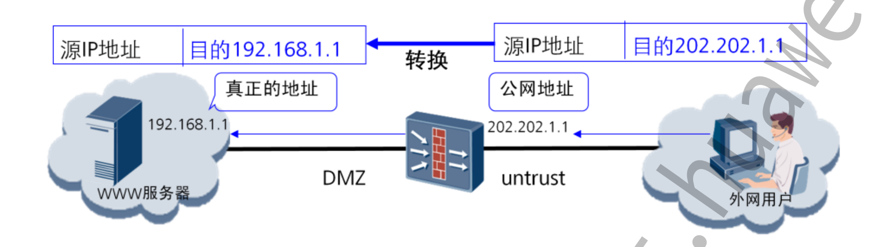


目录



NAT Server-内部服务器

- 内部服务器(Nat Server)功能是使用一个公网地址来代表内部服务器对外地址。



- 在防火墙上，专门为内部的服务器配置一个对外的公网地址来代表私网地址。对于外网用户来说，防火墙上配置的外网地址就是服务器的地址。

 Page 21



NAT Server，即内部服务器。NAT隐藏了内部网络的结构，具有“屏蔽”内部主机的作用。但是在实际应用中，可能需要提供给外部一个访问内部主机的机会，如提供给外部一台WWW的服务器，而外部主机根本没有指向内部地址的路由，因此无法正常访问。这时可以使用内部服务器（Nat Server）功能来实现这个功能应用。

使用NAT可以灵活地添加内部服务器。例如：可以使用202.202.1.1等公网地址作为Web服务器的外部地址，甚至还可以使用202.202.1.1 :8080这样的IP地址加端口号的方式作为Web的外部地址。

外部用户访问内部服务器时，有如下两部分操作：

- 防火墙将外部用户的请求报文的目的地址转换成内部服务器的私有地址。
- 防火墙将内部服务器的回应报文的源地址（私网地址）转换成公网地址。

防火墙支持基于安全区域的内部服务器。例如，当需要对处于多个网段的外部用户提供访问服务时，防火墙结合安全区域配置内部服务器可以为一个内部服务器配置多个公网地址。通过配置防火墙的不同级别的安全区域对应不同网段的外部网络，并根据不同安全区域配置同一个内部服务器对外的不同的公网地址，使处于不同网段的外部网络访问同一个内部服务器时，即通过访问对应配置的公网地址来实现对内部服务器的访问能力。

基于NAT Server的配置（命令行）

- 在系统视图下:

nat server [*id*] **protocol** *protocol-type* **global** { *global-address* [*global-address-end*] | **interface** *interface-type interface-number* } **inside** *host-address* [*host-address-end*] [**vrrp** { *virtual-router-id* | **master** | **slave** }] [**no-reverse**] …



 Page 22



NAT Server是最常用的基于目的地址的NAT。当内网部署了一台服务器，其真实IP是私网地址，但是希望公网用户可以通过一个公网地址来访问该服务器，这时可以配置NAT Server，使设备将公网用户访问该公网地址的报文自动转发给内网服务器。

针对配置NAT Server ，有以下不同类型:

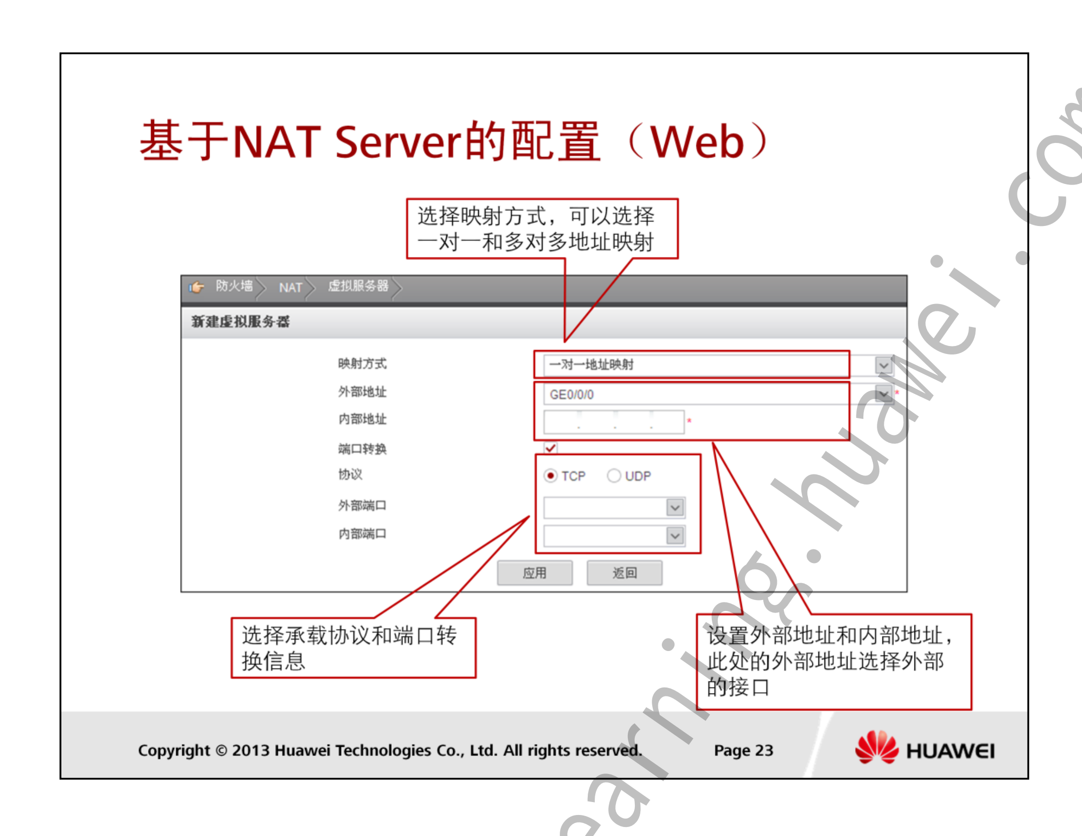
对所有安全区域发布同一个公网IP，即这些安全区域的用户都可以通过访问同一个公网IP来访问内部服务器。

与发布不同的公网IP相比，发布同一个公网IP地址时多了个参数*no-reverse*。配置不带*no-reverse*参数的**nat server**后，当公网用户访问服务器时，设备能将服务器的公网地址转换成私网地址；同时，当服务器主动访问公网时，设备也能将服务器的私网地址转换成公网地址。

参数*no-reverse*表示设备只将公网地址转换成私网地址，不能将私网地址转换成公网地址。当内部服务器主动访问外部网络时需要执行outbound的nat策略，引用的地址池里必需是nat server配置的公网IP地址，否则反向NAT地址与正向访问的公网IP地址不一致，会导致网络连接失败。

多次执行带参数*no-reverse*的**nat server**命令，可以为该内部服务器配置多个公网地址；未配置参数*no-reverse*则表示只能为该内部服务器配置一个公网地址。

针对不同的安全区域发布不同的公网IP，即不同安全区域的用户可以通过访问不同的公网IP来访问内部服务器。适用于内部服务器向不同的运营商网络提供服务，且在每个运营商网络都拥有一个公网IP的情况。



在Web配置界面中，配置NAT Server的配置步骤如下：

1. 选择“防火墙 > NAT > 虚拟服务器”。
2. 在“虚拟服务器列表”中，单击“新建”。
3. 依次输入或选择各项参数。

映射方式一共有三种方式可选，一对一地址映射、内部地址映射外部端口、内部地址映射外部地址：

- 一对一地址映射

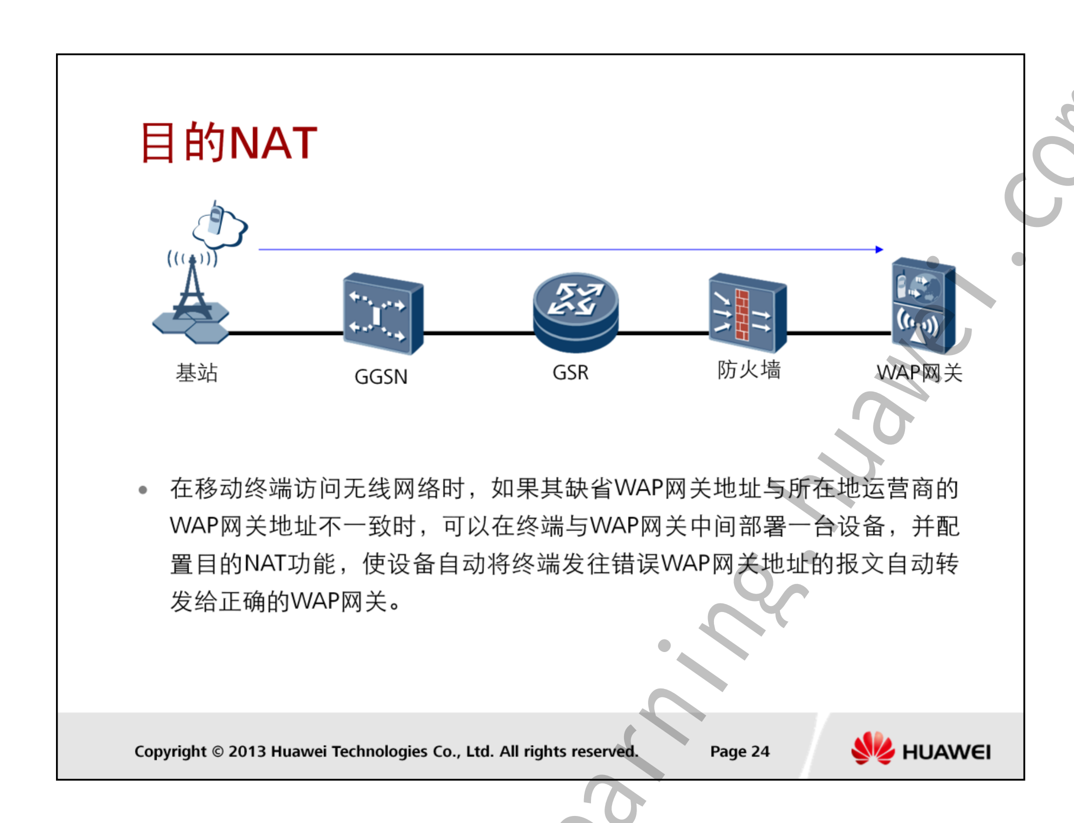
此种方式，将内部地址和外部地址进行一对一映射，内部地址的端口和外部地址的端口也进行一对一映射。

- 内部地址映射外部端口

此种方式，将内部地址（单个IP或者网段）映射为一个外部地址。当内部地址为单个IP时，外部地址对应一个外部端口；当内部地址为一个网段时，外部地址对应配置相同数量范围的外部端口。

- 内部地址映射外部地址

此种方式，将同网段内的内网服务器地址映射为相同数量且连续的公网IP地址，端口转换为可选配置，内部端口和外部端口都只能配置一个端口。



手机用户需要通过登录WAP（Wireless Application Protocol）网关来实现上网的功能。目前，大量用户使用直接从国外购买的手机，这些手机出厂时，缺省设置的WAP网关地址与本国WAP网关地址不符，且无法自行修改，从而导致用户不能移动上网。为解决这一问题，无线网络中，在WAP网关与用户之间部署防火墙。通过在设备上配置目的NAT功能，使这部分手机用户能够正常获取网络资源。

当手机用户上网时，目的NAT处理过程如下：

1. 当手机用户上网时，请求报文经过基站及其他中间设备到达防火墙。
2. 到达防火墙的报文如果匹配防火墙上所配置的目的NAT策略，则将此数据报文的目的IP地址转换为已配置好的WAP网关的IP地址，并送往WAP网关。
3. WAP网关对手机客户端提供相应的业务服务（如视频服务、网页服务等），并将回应报文发往防火墙。
4. 回应报文在防火墙上命中会话，防火墙转换该报文的源IP地址，并将该报文发往手机用户，完成一次通信。

这里我们可以把WAP网关理解为代理服务器。

基于目的NAT的配置（命令行）

- 在系统视图下，进入安全区域视图，配置目的NAT

  firewall zone [**name**] *zone-name*

  destination-nat *acl-number* **address** *ip-address* [**port** *port-number*]

- 举例：

  [USG] firewall zone trust

  [USG-zone-trust] destination-nat 3333 address 202.1.1.2

 Page 25



目的NAT，是通过ACL标识需转发目的IP地址的数据流，ACL是达成此应用场景的关键，即需要了解目前WAP网关IP地址有哪些，然后再通过ACL对WAP网关IP地址进行定义。

备注：目的NAT不支持与NAT ALG同时使用。

此处的ACL，应该严格配置，避免非WAP业务数据流被destination-nat命令引用，从而导致非WAP业务中断。

此处只能引用范围为3000～3999的高级ACL。

基于目的NAT的配置（Web）

源安全区域通常为用户所属的安全区域。源地址为来自源安全区域的报文的源IP地址。

防火墙 > NAT > 目的NAT

新建目的NAT策略

源安全区域	trust
源地址	any
目的地址	any
服务	ip
时间段	all
动作	permit
转换后的IP地址	. . .
转换后的端口	<1-50000>

应用 返回

配置转换后的IP地址通常为本地运营商的WAP网关的IP地址

 Page 26 HUAWEI

在Web配置界面中，基于目的的NAT配置步骤如下：

1. 选择“防火墙 > NAT > 目的NAT”。
2. 在“目的NAT策略列表”中，单击“新建”。
3. 依次输入或选择各项参数。

在配置参数中，源安全区域通常为用户所属的安全区域，转换后的IP地址为目的IP地址，通常为本地运营商的WAP网关的IP地址。



目录



双向NAT技术

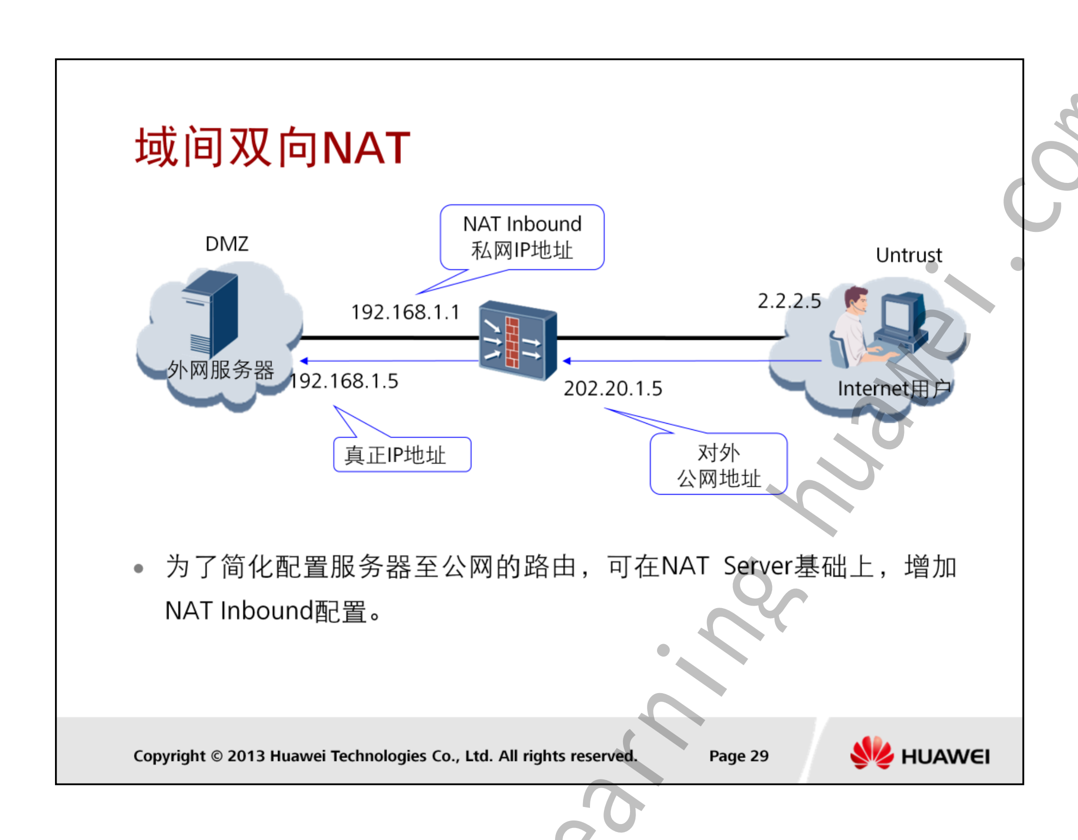
- 双向NAT两种应用场景:
  - NAT Server + NAT Inbound
  - NAT Server + 域内NAT

 Page 28 HUAWEI

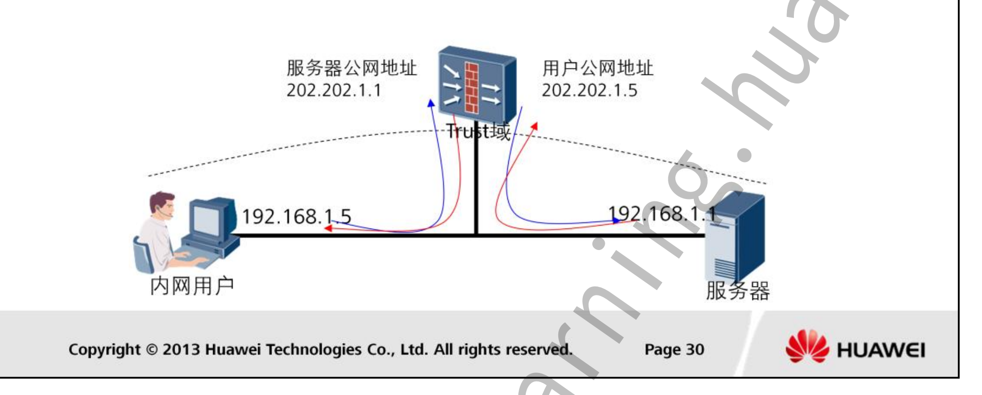
双向NAT应用场景的通信双方访问对方的时候目的地址都不是真实的地址，而是NAT转换后的地址。而outbound方向、inbound方向、内部服务器等应用都是只是针对某一方来进行地址转换。

一般来说，内网属于高优先级区域，外网属于低优先级区域。当低优先级安全区域的外网用户访问内部服务器的公网地址时，会将报文的目的地址转换为内部服务器的私网地址，但内部服务器需要配置到该公网地址的路由。

如果要避免配置到公网地址的路由，则可以配置从低优先级安全区域到高优先级安全区域方向的NAT，即inbound 方向的NAT。同一个安全区域内的访问需要作NAT，则需要配置域内NAT功能。



当配置NAT Server时，服务器需要配置到公网地址的路由才可正常发送回应报文。如果要简化配置，避免配置到公网地址的路由，则可以对外网用户的源IP地址也进行转换，转换后的源IP地址与服务器的私网地址在同一网段。这样内部服务器会缺省将回应报文发给网关，即设备本身，由设备来转发回应报文。由于外网安全区域的安全级别一般比内网低，所以这种应用又称为NAT Inbound。



若需要地址转换的双方都在同一个安全域内，那么就涉及到了域内NAT的情况。当FTP服务器和用户均在Trust区域，用户访问FTP服务器的对外的公网IP地址，这样用户与FTP服务器之间所有的交互报文都要经过防火墙。这时需要同时配置内部服务器和域内NAT。

域内NAT是指当内网用户和服务器部署在同一安全区域的情况下，仍然希望内网用户只能通过访问服务器的公网地址的场景。在实现域内NAT过程中，既要将访问内部服务器的报文的目的地址由公网地址转换为私网地址，又需要将源地址由私网地址转换为公网地址。



目录



NAT典型应用场景

Untrust 区域

202.169.10.1/29

Internet

192.168.20.1/24

DMZ 区域

192.168. 0 .1/24

Trust区域

- 应用场景分析
  - NAT Outbound应用
  - NAT Server应用

HUAWEI

防火墙NAT outbound配置(命令行)

- 配置域间访问规则。
  - 指定源地址为192.168.0.0网段。（具体配置步骤省略）
- 配置地址池。

  [USG]nat address-group 1 202.169.10.2 202.169.10.6
- 配置NAT Outbound策略

  [USG]**nat-policy interzone trust untrust outbound**

  [USG-nat-policy-interzone-trust-untrust-outbound]**policy 0**

  [USG-nat-policy-interzone-trust-untrust-outbound-0]**policy source 192.168.0.0 0.0.0.255**

  [USG-nat-policy-interzone-trust-untrust-outbound-0]**action source-nat**

  [USG-nat-policy-interzone-trust-untrust-outbound-0]**address-group 1**

Page 33



域间访问规则配置命令参考:

[USG]policy interzone trust untrust outbound

[USG-policy-interzone-trust-untrust-outbound]policy 0

[USG-policy-interzone-trust-untrust-outbound-0]policy source 192.168.0.0 0.0.0.255

[USG-policy-interzone-trust-untrust-outbound-0]action permit

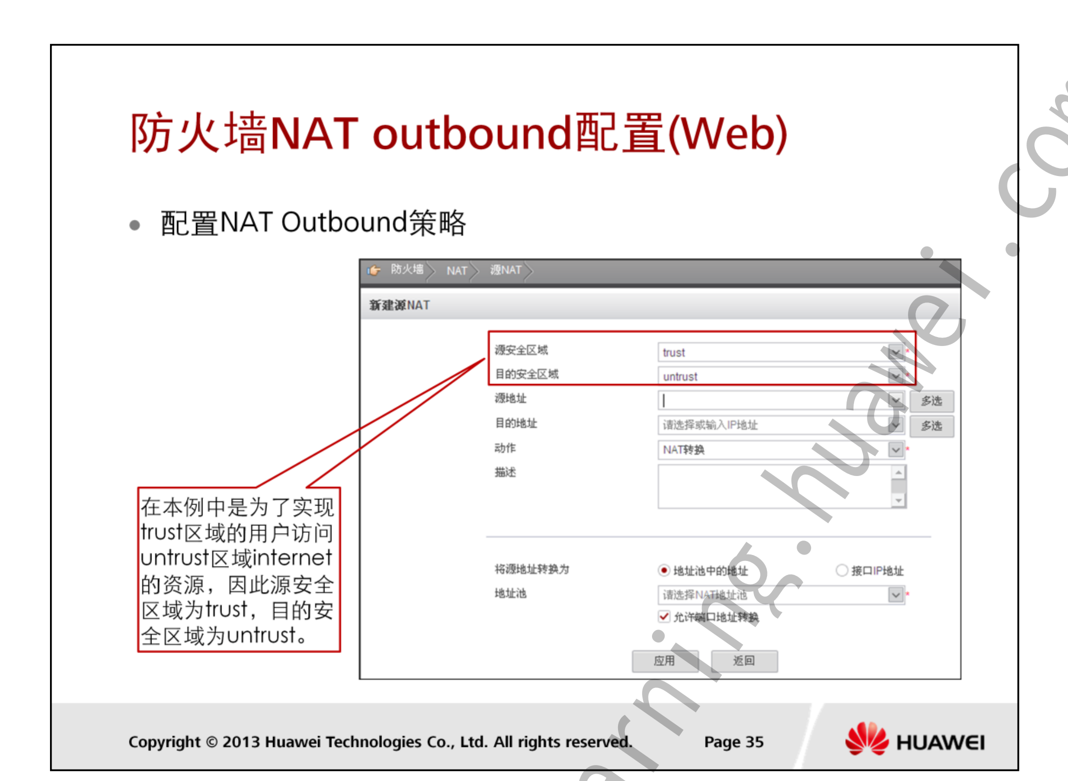
配置NAT outbound，是为了实现内网员工对外部网络进行访问时进行NAT地址转换，数据流向是从高安全级别到低安全级别，因此源地址应该为内部网络的地址网段。而为内网用户分配的地址池，应该为外网地址网段用于对internet资源进行访问。

防火墙NAT outbound配置(Web)

- 配置NAT 地址池



 Page 34 HUAWEI



源安全区域通常为转换前的私网IP地址所在的安全区域。在本例中为trust区域。目的安全区域通常为转换后的公网IP地址所在的安全区域。在本例中为untrust区域。

防火墙NAT Server配置(命令行)

- 配置内部Web和FTP服务器。

```
[USG] nat server protocol tcp global 202.169.10.1 80 inside 192.168.20.2 8080
[USG] nat server protocol tcp global 202.169.10.1 ftp inside 192.168.20.3 ftp
```

- 配置域间包过滤规则。

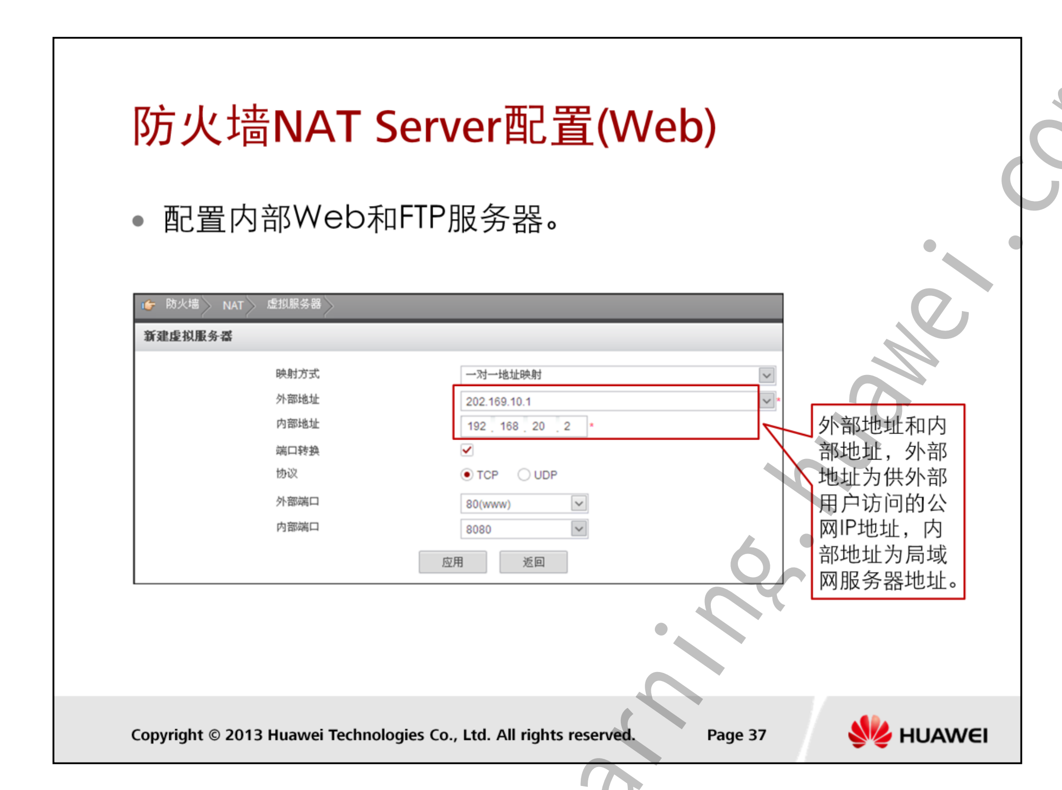
```
[USG] policy interzone dmz untrust  inbound
[USG-policy-interzone-dmz -untrust-inbound] policy 0
[USG-policy-interzone- dmz -untrust-inbound-0] policy destination 192.168.20.2  0
[USG-policy-interzone- dmz -untrust-inbound-0] policy service service-set http
[USG-policy-interzone- dmz -untrust-inbound-0] action permit
[USG-policy-interzone- dmz -untrust-inbound] policy 1
[USG-policy-interzone- dmz -untrust-inbound-1] policy destination 192.168.20.3  0
[USG-policy-interzone-dmz -untrust-inbound-1] policy service service-set ftp
[USG-policy-interzone- dmz -untrust-inbound-1] detect ftp
[USG-policy-interzone- dmz -untrust-inbound-1] action permit
```

 Page 36



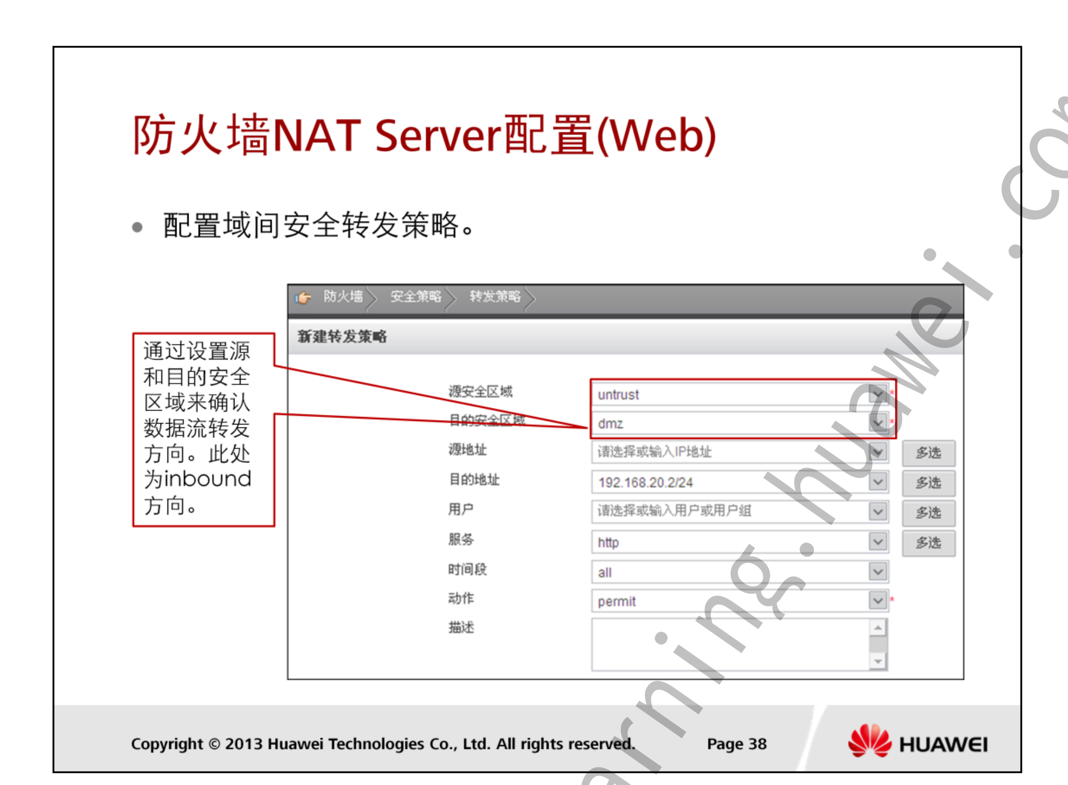
USG上同时配置NAT和内部服务器时，内部服务器优先级较高，首先起作用。

多个不同内部服务器使用一个公有地址对外发布时，可以多次使用 nat server 命令对其进行配置。配置参数 zone，可以使内部服务器访问该 zone 时候做 NAT 服务器逆向转换。当一个用户和内部服务器处于同一安全区域时，USG统一安全网关允许该用户使用内部服务器的公网IP地址访问该内部服务器。允许外部网络访问的内部服务器通常置于 USG 统一安全网关的 DMZ安全区域。不建议配置允许这个安全区域中的设备主动向外发起连接。当统一安全网关同时应用于双机热备组网时，如果转换后的 NAT 服务器地址与 VRRP备份组虚拟 IP地址不在同一网段，则不必配置携带 vrrp关键字的 nat server 命令。如果转换后的 NAT 服务器地址与 VRRP备份组的虚拟 IP地址在同一网段，则需要配置相关命令，且virtual-router-ID为统一安全网关 NAT 服务器出接口对应的 VRRP备份组的ID。



配置NAT Server时，外部地址为内部服务器提供给外部用户访问的公网IP地址。

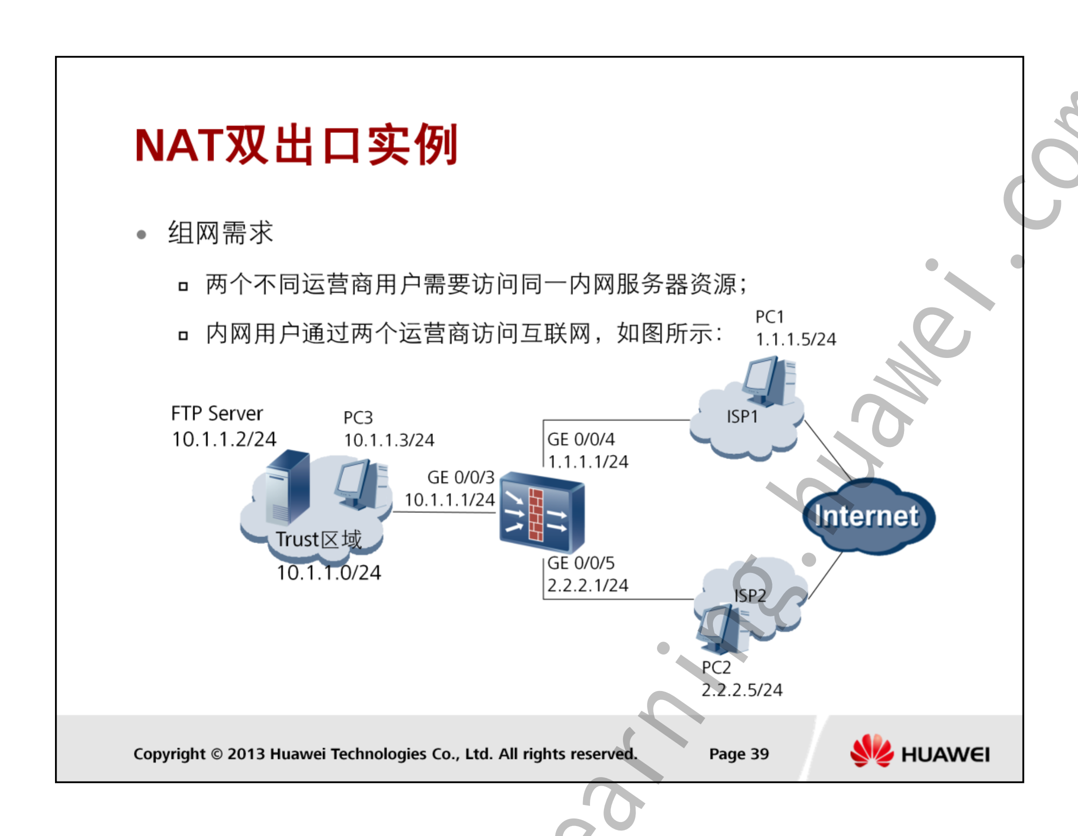
内部地址为内部服务器在局域网中的IP地址。



在Web配置界面中，配置域间包过滤规则的步骤为：

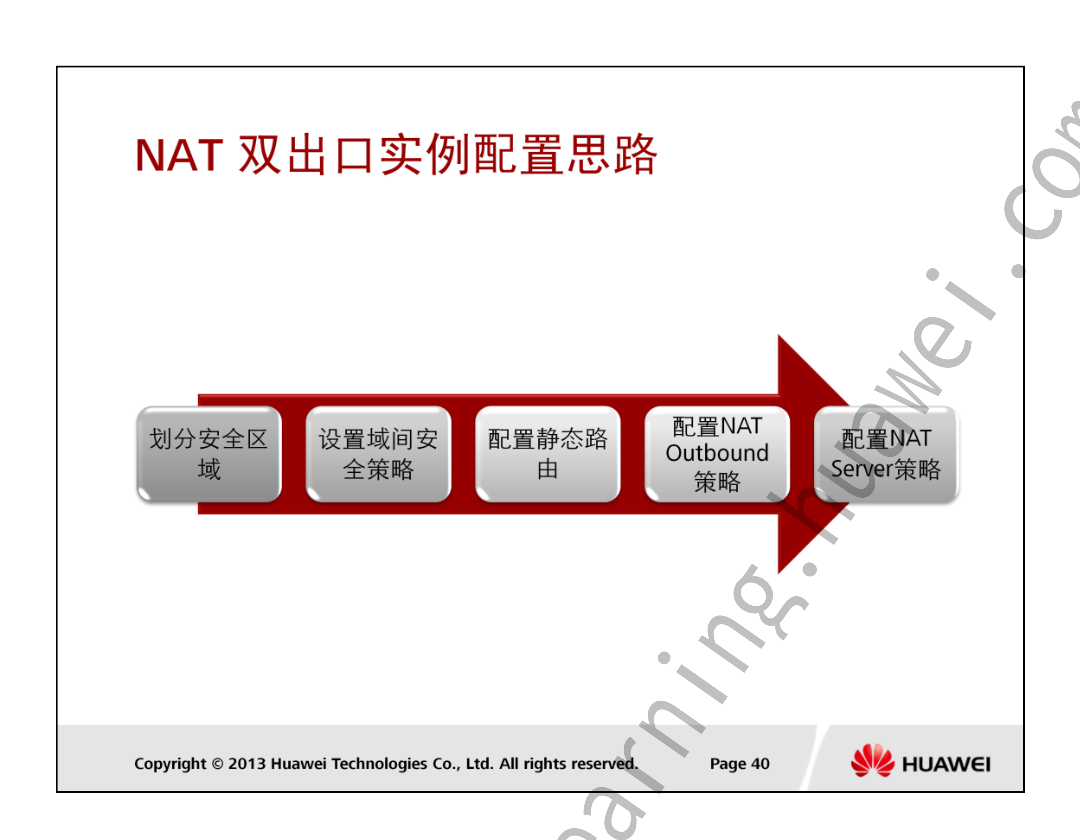
1. 选择“防火墙 > 安全策略 > 转发策略”。
2. 在“转发策略列表”中，单击“新建”。
3. 依次输入或选择各项参数。

使用Web配置方式配置域间安全转发策略时，没有单独的地方指定inbound或outbound方向，因此需要确定源安全区域和目的安全区域来区分数据流方向。



在该例中，这个企业从每个运营商处都获取到了一个公网IP地址，为了保证所有用户的访问速度，需要让不同运营商的用户通过访问相应的运营商的IP来访问公司提供的服务，而不需要经过运营商之间的中转。同时，对于企业内网的用户也可以通过两个运营商所提供的网络访问到internet资源。

ISP1和ISP2作为internet运营商，两者都连接internet并可以互通。



配置静态路由以实现从内网用户资源到达ISP1和ISP2的路由可达。

NAT Outbound双出口配置1（命令行）

- 创建安全区域。 为ISP1和ISP2分别创建一个安全区域。
  - [USG] **firewall zone name ISP1**
  - [USG-zone-isp1] **set priority 10**
  - [USG] **firewall zone name ISP2**
  - [USG-zone-isp2] **set priority 20**
- 配置各接口的IP地址，并将其加入相应的安全区域。 （配置省略）
- 配置域间安全转发策略。开启内网到ISP1和ISP2区域的outbound方向策略
  - [USG] **policy interzone trust isp1 outbound**
  - [USG-policy-interzone-trust-isp1-inbound] **policy 0**
  - [USG-policy-interzone-trust-isp1-inbound-0] **policy destination 1.1.1.5 0**
  - [USG-policy-interzone-trust-isp1-inbound-0] **action permit**

 Page 41



配置各接口的IP地址，并将其加入安全区域。配置命令参考：

[USG] interface GigabitEthernet 0/0/3

[USG-GigabitEthernet0/0/3] ip address 10.1.1.1 24

[USG] interface GigabitEthernet 0/0/4

[USG-GigabitEthernet0/0/4] ip address 1.1.1.1 24

[USG-GigabitEthernet0/0/4] quit

[USG] interface GigabitEthernet 0/0/5

[USG-GigabitEthernet0/0/5] ip address 2.2.2.1 24

[USG]firewall zone trust

[USG-zone-trust]add interface gigabitetherent 0/0/3

[USG]firewall zone isp1

[USG-zone-isp1]add interface gigabitetherent 0/0/4

[USG]firewall zone isp2

[USG-zone-isp2]add interface gigabitetherent 0/0/5

NAT Outbound双出口配置2（命令行）

- 配置静态路由，保证路由可达 。

  假设通过ISP1和ISP2访问internet资源的下一跳地址分别为1.1.1.2/24和2.2.2.2/24。

  （具体步骤省略）

- 配置NAT Outbound策略 （isp2策略步骤省略）

  [USG]**nat-policy interzone trust isp1 outbound**

  [USG-nat-policy-interzone-trust-untrust-outbound]**policy 0**

  [USG-nat-policy-interzone-trust-untrust-outbound-0]**action source-nat**

  [USG-nat-policy-interzone-trust-untrust-outbound-0]**easy-ip GigabitEthernet 0/0/4**

 Page 42



静态路由配置命令参考：

[USG] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2

[USG] ip route-static 0.0.0.0 0.0.0.0 2.2.2.2

NAT Server双出口配置1（命令行）

- 配置域间安全转发策略。开启内网到ISP1和ISP2区域的inbound方向策略
  - （ISP2的配置与ISP1相似，具体配置省略）

[USG] **policy interzone trust isp1 inbound**

[USG-policy-interzone-trust-isp1-inbound] **policy 0**

[USG-policy-interzone-trust-isp1-inbound-0] **policy destination 10.1.1.3 0**

[USG-policy-interzone-trust-isp1-inbound-0] **policy service service-set ftp**

[USG-policy-interzone-trust-isp1-inbound-0] **action permit**

 Page 43 

配置接口IP地址、接口加域配置命令参考：

<USG> system-view

[USG] interface GigabitEthernet 0/0/3

[USG-GigabitEthernet0/0/3] ip address 10.1.1.1 24

[USG-GigabitEthernet0/0/3] quit

[USG] interface GigabitEthernet 0/0/4

[USG-GigabitEthernet0/0/4] ip address 1.1.1.1 24

[USG-GigabitEthernet0/0/4] quit

[USG] interface GigabitEthernet 0/0/5

[USG-GigabitEthernet0/0/5] ip address 2.2.2.1 24

[USG-GigabitEthernet0/0/5] quit

[USG] firewall zone dmz

[USG-zone-dmz] add interface GigabitEthernet 0/0/3

[USG-zone-dmz] quit

[USG] firewall zone untrust

[USG-zone-untrust] add interface GigabitEthernet 0/0/4

[USG-zone-untrust] add interface GigabitEthernet 0/0/5

[USG-zone-untrust] quit

NAT Server双出口配置2（命令行）

- 创建内网服务器的公网IP与私网IP的映射关系。

  [USG] **nat server zone isp1 protocol tcp global 1.1.1.1 ftp inside 10.1.1.2 ftp**

  [USG] **nat server zone isp2 protocol tcp global 2.2.2.1 ftp inside 10.1.1.2 ftp**

- 在ISP1、ISP2与DMZ的域间配置NAT ALG，使服务器可以正常对外提供FTP服务。

  [USG] **firewall interzone dmz isp1**

  [USG-interzone-dmz-isp1] **detect ftp**

  [USG-interzone-dmz-isp1] **quit**

  [USG] **firewall interzone dmz isp2**

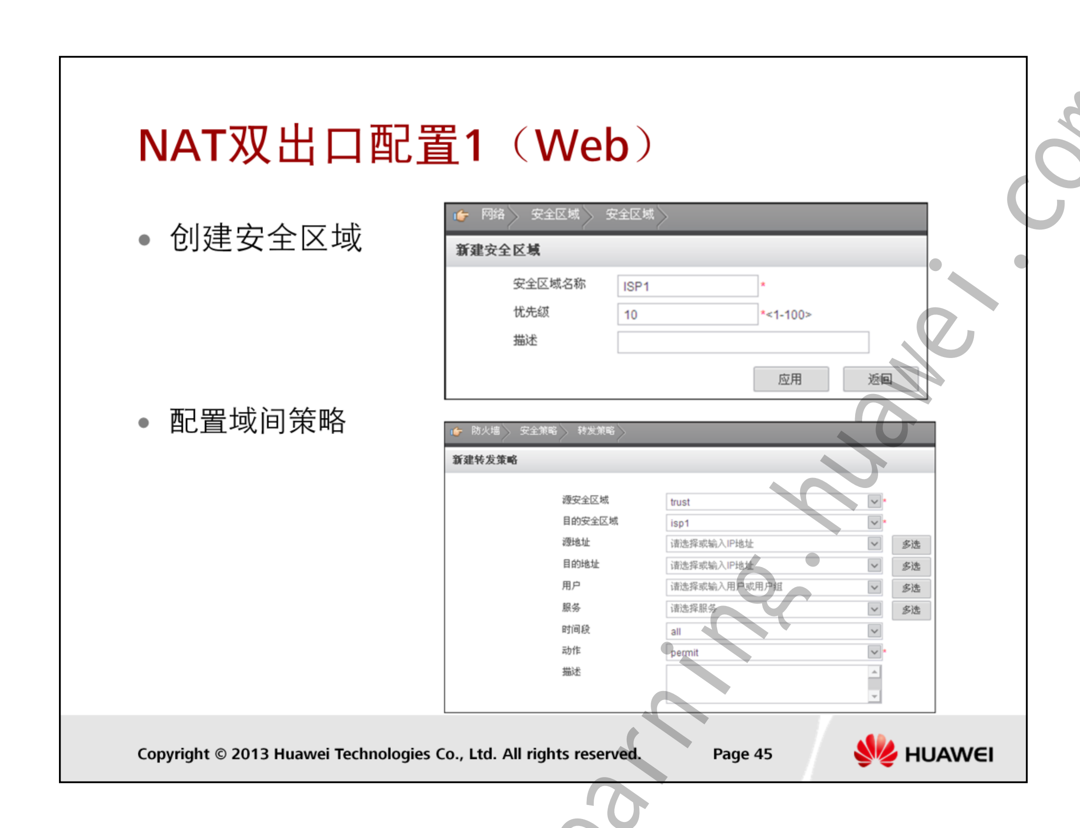
  [USG-interzone-dmz-isp2] **detect ftp**

  [USG-interzone-dmz-isp2] **quit**

 Page 44



在本例中，ISP1和ISP2可以划为同一安全区域也可以设置为不同的安全区域。在这种时候，需要采用nat server zone 方式可以使防火墙识别报文“来自”或者“去往”的域，对报文的目的地址和源地址通过nat server所创建的地址映射关系进行转换。



在Web配置界面中，创建安全区域的操作步骤为：

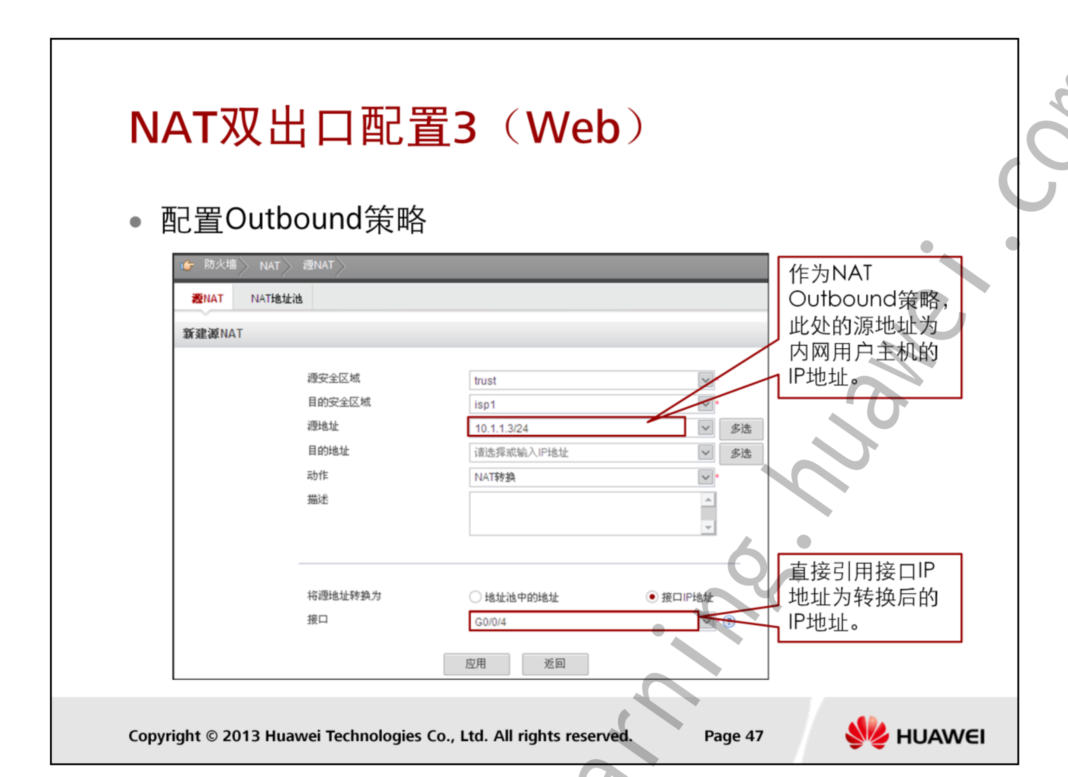
1. 选择“网络 > 安全区域 > 安全区域”。
2. 单击“安全区域列表”中的“新建”。
3. 依次输入各项参数。

安全区域名称和优先级一旦设定，便不允许更改，同时不能与系统已存在的安全区域名称和优先级相同。



在Web配置界面中，配置静态路由的步骤为：

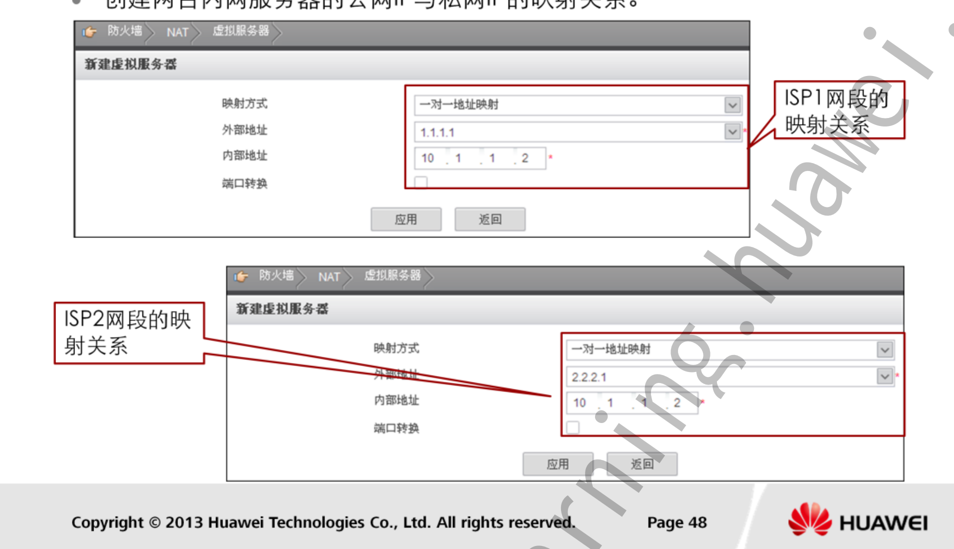
1. 选择“路由 > 静态 > 静态路由”。
2. 在“静态路由列表”中，单击“新建”。
3. 依次输入或选择各项参数。



在如图所示的配置中，设置了从内网用户10.1.1.3到ISP1网段的NAT outbound策略，内网用户转换后的IP地址为到ISP1的接口G0/0/4的IP地址，此种转换方式相当于命令行中easy IP的方式。

NAT双出口配置4（Web）

- 创建两台内网服务器的公网IP与私网IP的映射关系。



  HUAWEI



总结

- NAT的技术原理
- NAT几种应用方式
- 防火墙NAT典型场景配置



思考题

- NAT Inbound与NAT Outbound有何区别?
- No-pat有哪些局限性?
- Easy-ip的应用场景是什么?
- 基于目的IP地址NAT中no-reverse参数的意义是什么?
- 域间双向NAT与域内双向NAT应用场景有何不同?
- NAT Server 双出口
- 在不同类型NAT应用场场景中，域间包过滤规则配置应注意哪些方面?



Thank you

www.huawei.com

HC110310005

HCNA-Security-CBSN 第五章 防火墙双机热备技术

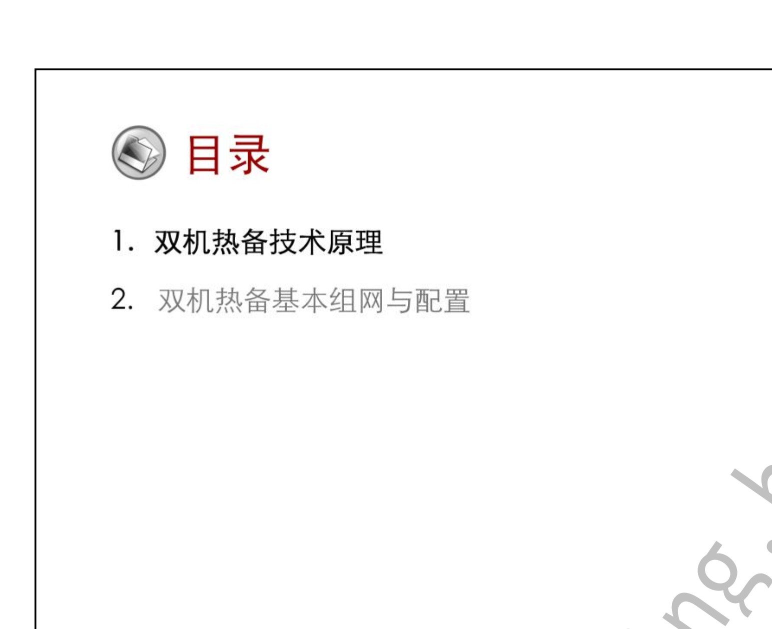

第五章
防火墙双机热备技术
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



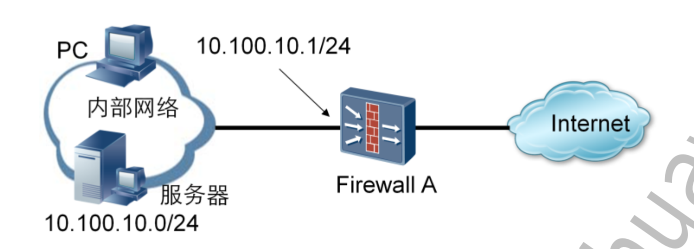
目标

- 学完本课程后，您将能够:
  - 掌握双机热备技术原理
  - 掌握双机热备基础配置




目录
1. 双机热备技术原理
2. 双机热备基本组网与配置
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 2
HUAWEI

双机热备份技术产生的原因

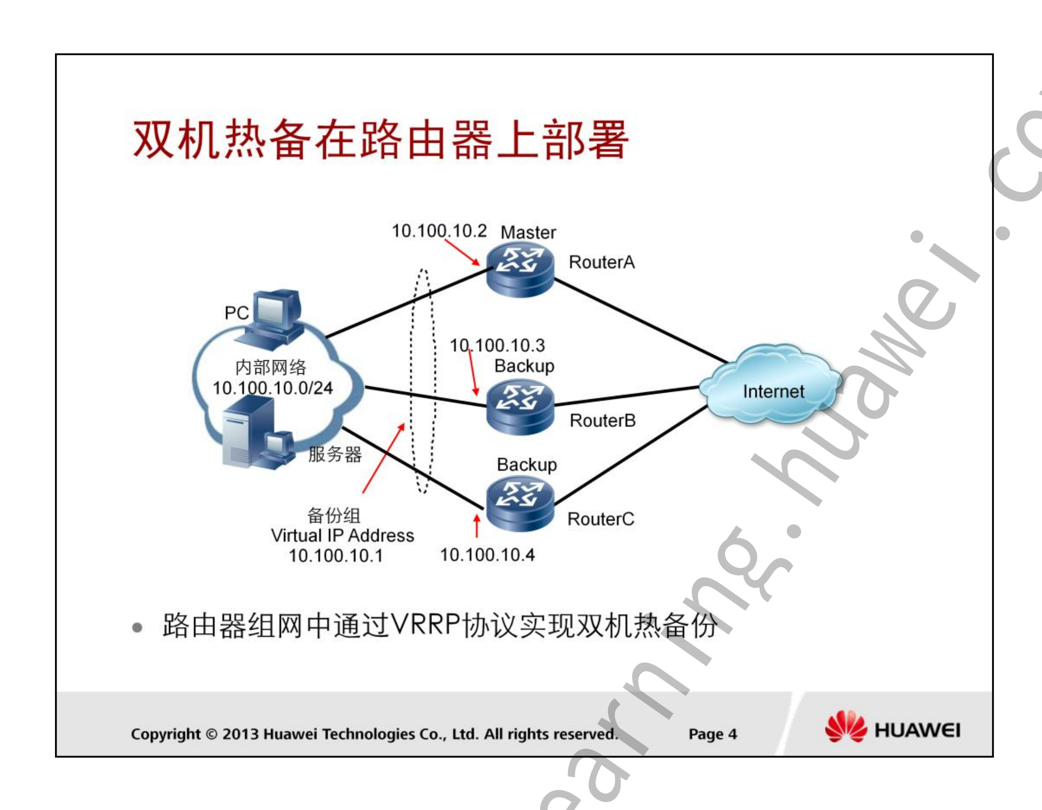


- 传统的组网方式如图所示，内部用户和外部用户的交互报文全部通过Firewall A。如果Firewall A出现故障，内部网络中所有以Firewall A作为默认网关的主机与外部网络之间的通讯将中断，通讯可靠性无法保证。

 Page 3 

双机热备份技术的出现改变了可靠性难以保证的尴尬状态，通过在网络出口位置部署两台或多台网关设备，保证了内部网络于外部网络之间的通讯畅通。

USG防火墙作为安全设备，一般会部署在需要保护的网络和不受保护的网络之间，即位于业务接口点上。在这种业务点上，如果仅仅使用一台USG防火墙设备，无论其可靠性多高，系统都可能会承受因为单点故障而导致网络中断的风险。为了防止一台设备出现意外故障而导致网络业务中断，可以采用两台防火墙形成双机备份。

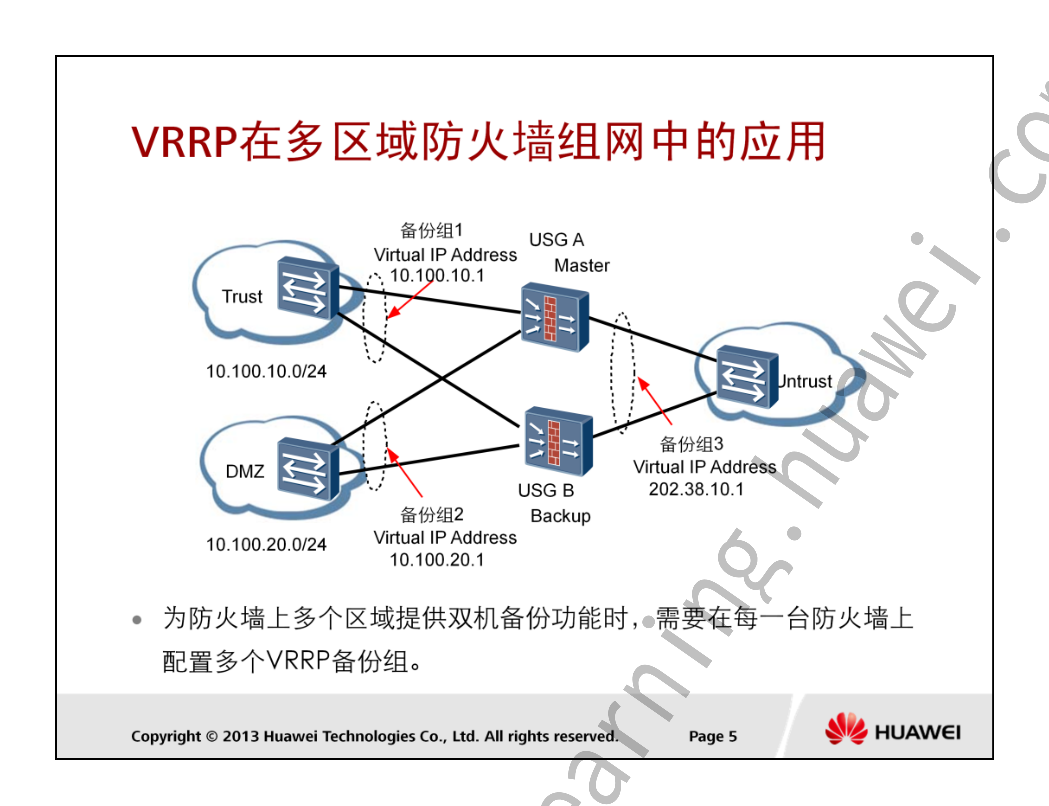


为了避免路由器传统组网所引起的单点故障的发生，通常情况可以采用多条链路的保护机制，依靠动态路由协议进行链路切换。但这种路由协议来进行切换保护的方式存在一定的局限性，当不能使用动态路由协议时，仍然会导致链路中断的问题，因此推出了另一种保护机制VRRP（虚拟路由冗余协议）来进行。采用VRRP的链路保护机制比依赖动态路由协议的广播报文来进行链路切换的时间更短，同时弥补了不能使用动态路由情况下的链路保护。

VRRP（Virtual Router Redundancy Protocol）是一种基本的容错协议。

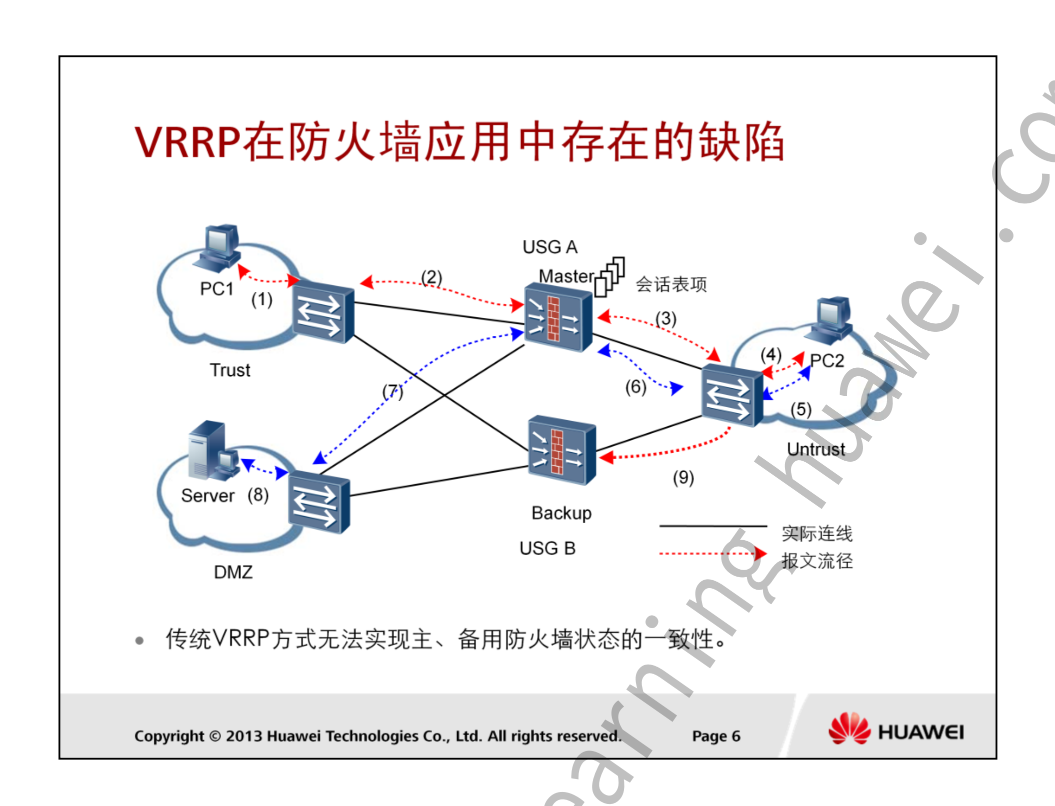
- 备份组：同一个广播域的一组路由器组织成一个虚拟路由器，备份组中的所有路由器一起，共同提供一个虚拟IP地址，作为内部网络的网关地址。
- 主（Master）路由器：在同一个备份组中的多个路由器中，只有一台处于活动状态，只有主路由器能转发以虚拟IP地址作为下一跳的报文。
- 备份（Backup）路由器：在同一个备份组中的多个路由器中，除主路由器外，其他路由器均为备份路由器，处于备份状态。

主路由器通过组播方式定期向备份路由器发送通告报文（HELLO），备份路由器则负责监听通告报文，以此来确定其状态。由于VRRP HELLO报文为组播报文，所以要求备份组中的各路由器通过二层设备相连，即启用VRRP时上下行设备必须具有二层交换功能，否则备份路由器无法收到主路由器发送的HELLO报文。如果组网条件不满足，则不能使用VRRP。



当防火墙上多个区域需要提供双机备份功能时，需要在一台防火墙上配置多个VRRP备份组。

由于USG防火墙是状态防火墙，它要求报文的来回路径通过同一台防火墙。为了满足这个限制条件，就要求在同一台防火墙上的所有VRRP备份组状态保持一致，即需要保证在主防火墙上所有VRRP备份组都是主状态，这样所有报文都将从此防火墙上通过，而另外一台防火墙则充当备份设备。



如图所示，假设USG A和USG B的VRRP状态一致，即USG A的所有接口均为主用状态，USG B的所有接口均为备用状态。

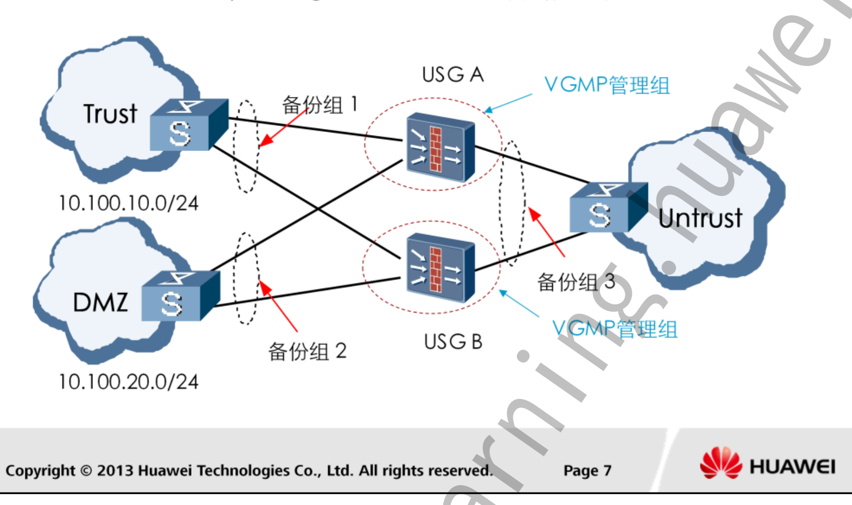
此时，Trust区域的PC1访问Untrust区域的PC2，报文的转发路线为(1)-(2)-(3)-(4)。USG A转发访问报文时，动态生成会话表项。当PC2的返回报文经过(4)-(3)到达USG A时，由于能够命中会话表项，才能再经过(2)-(1)到达PC1，顺利返回。同理，当PC2和DMZ区域的Server也能互访。

假设USG A和USG B的VRRP状态不一致，例如，当USG B与Trust区域相连的接口为备用状态，但与Untrust区域的接口为主用状态，则PC1的报文通过USG A设备到达PC2后，在USG A上动态生成会话表项。PC2的返回报文通过路线(4)-(9)返回。此时由于USG B上没有相应数据流的会话表项，在没有其他报文过滤规则允许通过的情况下，USG B将丢弃该报文，导致会话中断。

问题产生的原因：报文的转发机制不同。

- 路由器：每个报文都会查路由表当匹配上后才进行转发，当链路切换后，后续报文不会受到影响，继续进行转发。
- 状态检测防火墙：如果首包允许通过会建立一条五元组的会话连接，只有命中该会话表项的后续报文（包括返回报文）才能够通过防火墙；如果链路切换后，后续报文找不到正确的表项，会导致业务中断。

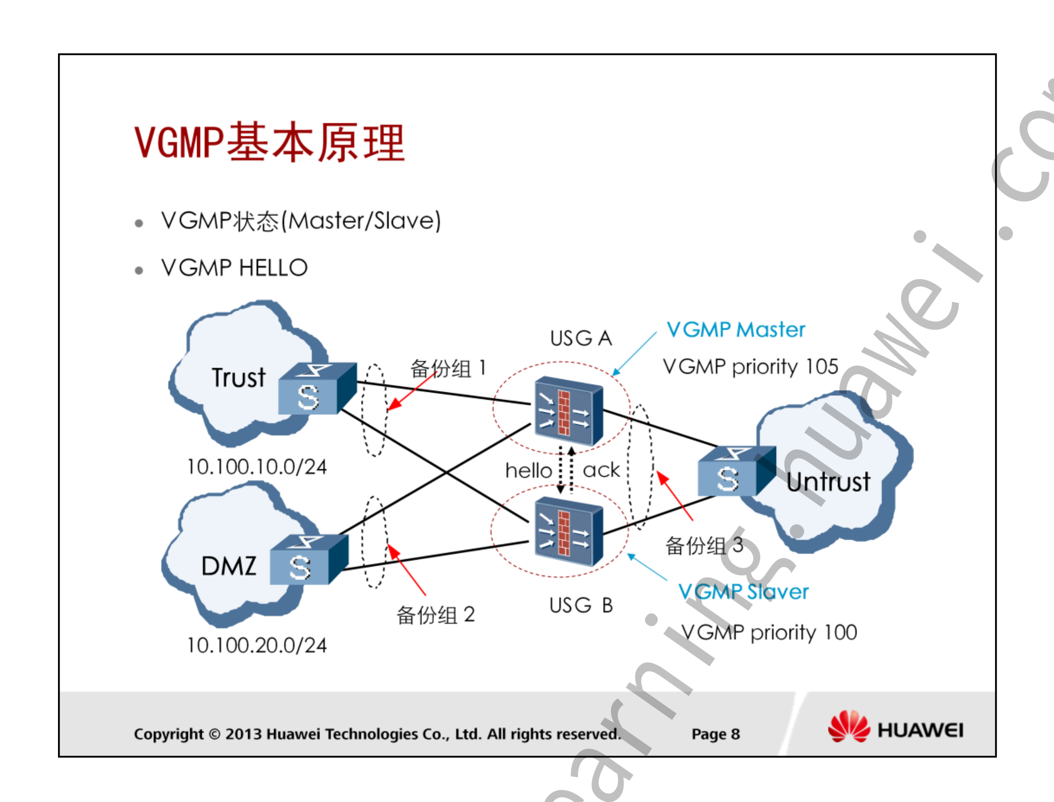
注意：当路由器配置NAT后也会存在同样的问题，因为在进行NAT后会形成一个NAT转换后的表项。



VRRP在防火墙中应用的要求：

- VRRP状态的一致性
- 会话表状态备份

VGMP提出VRRP管理组的概念，将同一台防火墙上的多个VRRP备份组都加入到一个VRRP管理组，由管理组统一管理所有VRRP备份组。通过统一控制各VRRP备份组状态的切换，来保证管理组内的所有VRRP备份组状态都是一致的。



当防火墙上的VGMP为Master状态时，组内所有VRRP备份组的状态统一为Master状态，所有报文都将从该防火墙上通过，该防火墙成为主用防火墙。此时另外一台防火墙上对应的VGMP为备状态，该防火墙成为备用防火墙。

通过指定VGMP组的优先级来决定谁将成为主防火墙或备用防火墙。

VGMP的优先级会根据组内的VRRP备份组成员的状态动态调整，以此完成两台防火墙的主备倒换。

与VRRP类似，状态为Master的VGMP也会定期向对端发送HELLO报文，通知Slave端本身的运行状态（包括优先级、VRRP成员状态等）。与VRRP不同的是，Slave端收到HELLO报文后，会回应一个ACK消息，该消息中也会携带本身的优先级、VRRP成员状态等。

VGMP HELLO报文发送周期缺省为1秒。当Slave端三个HELLO报文周期没有收到对端发送的HELLO报文时，会认为对端出现故障，从而将自己切换到Master状态。

VGMP组管理

- 状态一致性管理
  - VGMP管理组控制所有的VRRP备份组统一切换。
- 抢占管理
  - 当原来出现故障的主设备故障恢复时，其优先级也会恢复，此时可以重新将自己的状态抢占为主。

 Page 9



- 状态一致性管理

各备份组的主/备状态变化都需要通知其所属的VGMP管理组，由VGMP管理组决定是否允许VRRP备份组进行主/备状态切换。如果需要切换，则VGMP管理组控制所有的VRRP备份组统一切换。VRRP备份组加入到管理组后，状态不能自行单独切换。

- 抢占管理

VRRP备份组本身具有抢占功能。即当原来出现故障的主设备故障恢复时，其优先级也会恢复，此时可以重新将自己的状态抢占为主。

VGMP管理组的抢占功能和VRRP备份组类似，当管理组中出现故障的备份组故障恢复时，管理组的优先级也将恢复。此时VGMP可以决定是否需要重新抢占称为主设备。

当VRRP备份组加入到VGMP管理组后，备份组上原来的抢占功能将失效，抢占行为发生与否必须由VGMP管理组统一决定。

HRP基本概念

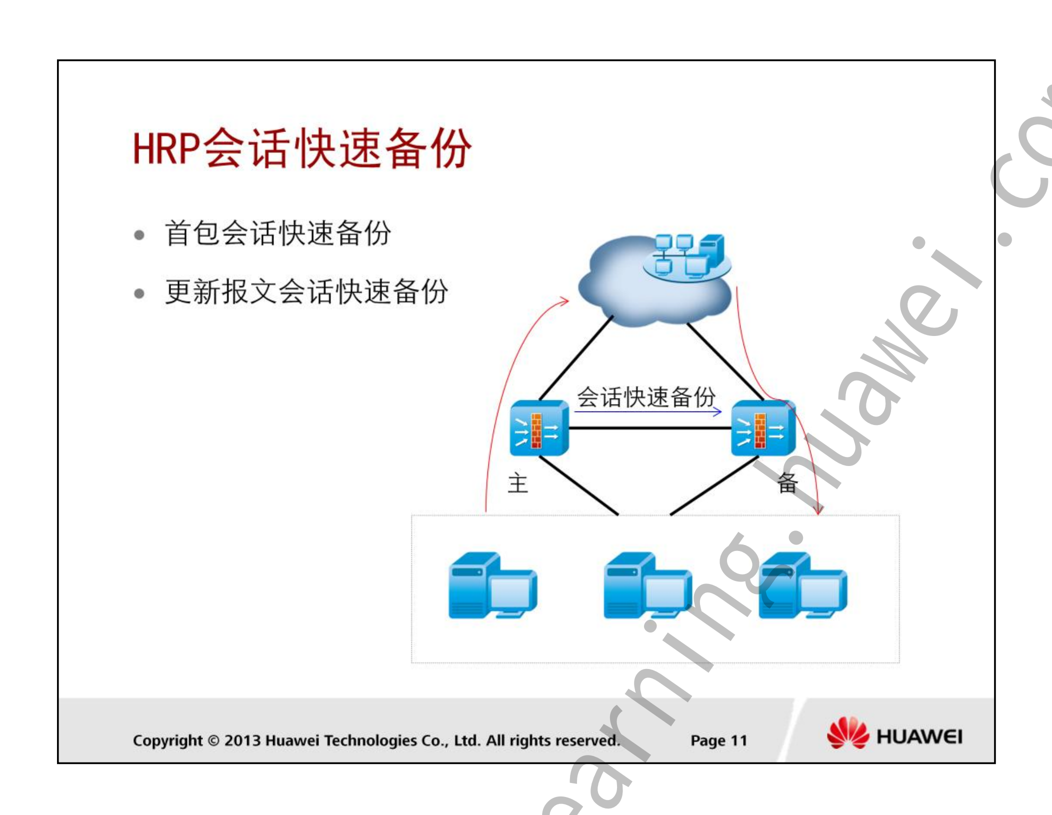
- HRP（Huawei Redundancy Protocol）协议，用来将主防火墙关键配置和连接状态等数据向备防火墙上同步。

 Page 10 HUAWEI

在双机热备组网中，当主防火墙出现故障时，所有流量都将切换到备防火墙。因为USG防火墙是状态防火墙，如果备防火墙上没有原来主防火墙上的会话表等连接状态数据，则切换到备防火墙的流量将无法通过防火墙，造成现有的连接中断，此时用户必须重新发起连接。

HRP模块提供了基础的数据备份机制和传输功能。各个应用模块收集本模块需要备份的数据，提交给HRP模块，HRP模块负责将数据发送到对端防火墙的对应模块，应用模块需要再将HRP模块提交上来的数据进行解析，并加入到防火墙的动态运行数据池中。

- 备份内容：要备份的连接状态数据包括TCP/UDP的会话表、ServerMap表项、动态黑名单、NO-PAT表项、ARP表项等。
- 备份方向:防火墙上有状态为主的VGMP管理组，向对端备份。
- 备份方式：分为三种
    - 批量备份：在两台设备第一次协商完成后，批量备份所有信息
    - 实时备份：在设备运行过程中，新建或者刷新的数据实时备份
    - 配置批量备份需要消耗较多的资源，缺省情况下是关闭的。
- 备份通道：一般情况下，在两台设备上直连的端口作为备份通道，有时也称为“心跳线”（VGMP也通过该通道进行通信）。



在来回路径不一致的组网中，业务流的来回报文有可能不会从同一个防火墙上经过。为了支持来回路径不一致的组网，防火墙增加了会话快速备份功能。即在首包创建会话时，立即将会话数据打包备份到对端，然后再将报文转发出去，保证了当回应的报文到达对端防火墙时，对端防火墙上已经接收到备份过来的会话数据并加入到会话表中。比如对于TCP三次握手的报文，SYN+ACK报文从另一台设备回来时，由于查不到会话，报文会被丢弃，导致连接建立失败。对于UDP会话，第一个反向报文过来时，在另一台上也会因为查不到会话，需要走包过滤流程，有可能会被丢弃。

通常情况下，对于TCP连接、状态改变的报文命中会话之后立即备份到对端，包括三次握手报文和fin、rst报文；对于UDP会话，快速备份是创建会话之后立即备份到对端，后续报文也进行备份以避免会话信息的老化。


目录
1. 双机热备技术原理
2. 双机热备基本组网与配置
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 12
HUAWEI

双机热备基本组网

- 上下行业务接口工作在三层模式，连接二层设备时，需要在上下行的业务接口上配置VRRP备份组，使VGMP管理组能够通过VRRP备份组监测三层业务接口。

Page 13
HUAWEI

双机热备组网最常见的是防火墙采用路由模式，下行交换机双线上联到防火墙，正常情况下防火墙A作为主，当防火墙A上行或下行链路down掉后，防火墙B自动切换为主设备，交换机流量走向防火墙B。

配置VRRP备份组

- 接口视图下配置VRRP：

  vrrp vrid *virtual-router-ID* virtual-ip *virtual-address [ip-mask* | *ip-mask-length] { master* | *slave }*

  - 执行此命令时，指定master或slave参数后，即将该VRRP组加入了VGMP管理组的Master或Slave管理组。
  - 每个普通物理接口（GigabitEthernet接口）下最多配置255个VRRP组。

 Page 14 

Master管理组默认情况下会每隔1秒发送一次vrrp报文，可以在接口视图下调整vrrp报文发送间隔。接口视图下修改vrrp报文发送时间：

vrrp vrid virtual-router-ID timer advertise adver-interval

vrrp也可以与ip-link进行配合，当上行链路断掉后使vrrp能够进行主备切换。在接口视图下配置ip-link：

vrrp vrid virtual-router-id ip-link link-id

缺省情况下，VGMP管理组的抢占功能为启用状态，抢占延迟时间为30s。配置VGMP管理组的抢占延迟时间命令如下：

hrp preempt [delay interval]

HRP配置命令

- 指定心跳口

  hrp interface *interface-type interface-number [remote { ip-address | ipv6-address }]*

- 启用HRP备份功能

  hrp enable

- 启用允许配置备用设备的功能

  hrp slave config enable

- 启用命令与状态信息的自动备份

  hrp auto-sync *[config | connection-status]*

- 启用会话快速备份

  hrp mirror session enable

 Page 15



HRP两台USG心跳口的接口类型和编号必须相同，且心跳口不能为二层以太网接口。USG支持使用Eth-Trunk接口做为心跳口，既提高了可靠性，又增加了备份通道的带宽。主备USG的心跳口可以直接相连，也可以通过中间设备，如交换机或路由器连接。当心跳口通过中间设备相连时，需要配置remote参数来指定对端IP地址。

当两台设启用备HRP备份功能之后，会进行主备状态的协商，最后得到一个主用设备（显示时以HRP_M表示），一个备用设备（显示时以HRP_S表示）。两端首次协商出主备后，主用设备将向备用设备备份配置和连接状态等信息。

启用允许配置备用设备的功能后，所有可以备份的信息都可以直接在备用设备上进行配置，且备用设备上的配置可以同步到主用设备。如果主备设备上都进行了某项配置，则从时间上来说，后配置的信息会覆盖先配置的信息。

USG工作于负载分担组网时，报文的来回路径可能会不一致，务必启用会话快速备份功能，使一台USG的会话信息立即同步至另一台USG，保证内外部用户的业务不中断。

VRRP配置举例

- USG_A关于VRRP组1配置：

  [USG_A]interface GigabitEthernet 0/0/0

  [USG_A-GigabitEthernet 0/0/0]ip address 10.100.10.2 24

  [USG_A-GigabitEthernet 0/0/0]vrrp vrid 1 10.100.10.1 master

- USG_B关于VRRP组1的配置：

  [USG_B]interface GigabitEthernet 0/0/0

  [USG_B-GigabitEthernet0/0/0]ip address 10.100.10.3 24

  [USG_B-GigabitEthernet 0/0/0]vrrp vrid 1 virtual-ip 10.100.10.1 slave



HRP配置举例

- USG_A关于HRP配置：

```
[USG_A]hrp enable
[USG_A]hrp mirror session enable
[USG_A]hrp interface Ethernet 2/0/0
[USG_A]hrp interface GigabitEthernet 0/0/0
[USG_A]hrp interface GigabitEthernet0/0/1
```


Page 17



USG_B关于HRP的配置：

```
[USG_B]hrp enable
[USG_B]hrp mirror session enable
[USG_B]hrp interface Ethernet 2/0/0
[USG_B]hrp interface GigabitEthernet 0/0/0
[USG_B]hrp interface GigabitEthernet 0/0/1
```

配置VRRP备份组——WEB方式

- 新建VRID组

HRP配置——WEB方式

- 配置双机热备
  - 启动HRP
  - 选择HRP备份通道





HUAWEI

HRP配置——WEB方式

- 双机热备高级配置选项

高级

☐ 启动会话快速备份　　☐ 允许配置备份设备
☑ 自动备份连接状态　　☑ 自动备份配置

手动备份连接状态　备份
手动备份配置　备份
检查HRP配置一致性　检查
检查ACL配置一致性　检查
配置HRP状态监控组　配置

抢占模式　☑ 主动抢占
抢占延时　30　*<0-1800>秒
Hello报文周期　1000　<500-60000>毫秒

设置OSPF Cost值　☐
备注:OSPF(Open Shortest Path First)是IETF组织开发的一个基于链路状态的内部网关协议，是一种用于自治系统AS（Autonomous System）内部的动态路由协议。

应用　刷新

HUAWEI

查看VRRP状态

```
HRP_M<USG_A>display vrrp int g0/0/1
  16:13:46  2013/06/08
   GigabitEthernet0/0/1 | Virtual Router 2
    VRRP Group : Master
    state : Master
    Virtual IP : 202.38.10.1
    Virtual MAC : 0000-5e00-0102
    Primary IP : 202.38.10.2
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
```






查看HRP状态

- 查看处于Master状态防火墙的状态信息如下：

HRP_M<USG_A>dis hrp state

16:15:31 2013/06/08

The firewall's config state is: MASTER

Current state of virtual routers configured as master:

GigabitEthernet0/0/1 vrid 2 : master

GigabitEthernet0/0/0 vrid 1 : master

Page 22



查看处于Slave状态防火墙的状态信息如下：

HRP_S[USG_B] display hrp state

16:40:13 2010/11/29

The firewall's config state is: SLAVE

Current state of virtual routers configured as slave:

GigabitEthernet0/0/0 vrid 1 : slave

GigabitEthernet0/0/1 vrid 2 : slave



总结

- 双机热备技术原理
- 双机热备基本组网及配置





习题

- 判断题
  1. HRP技术可以实现备防火墙不需要配置任何信息，所有配置信息均由主防火墙通过HRP同步至备防火墙，且重启后配置信息不丢失。
- 单选题
  1. 在防火墙做双机热备组网时，为实现备份组整体状态切换，需要使用以下哪个协议技术?

  A. VGMP　　B. VRRP　　C. HRP　　D. OSPF

Page 24



习题与答案:

1、HRP技术可以实现备防火墙不需要配置任何信息，所有配置信息均由主防火墙通过HRP同步至备防火墙，且重启后配置信息不丢失。

答案：错误

2、在防火墙做双机热备组网时，为实现备份组整体状态切换，需要使用以下哪个协议技术?

A. VGMP　　B. VRRP　　C. HRP　　D. OSPF

答案：A

Thank you

www.huawei.com

HC110310006

HCNA-Security-CBSN 第六章 防火墙用户管理

第六章

防火墙用户管理

www.huawei.com

HUAWEI



目标

- 学完本课程后，您将能够:
  - 掌握用户认证技术
  - 掌握AAA认证
  - 掌握用户认证管理配置



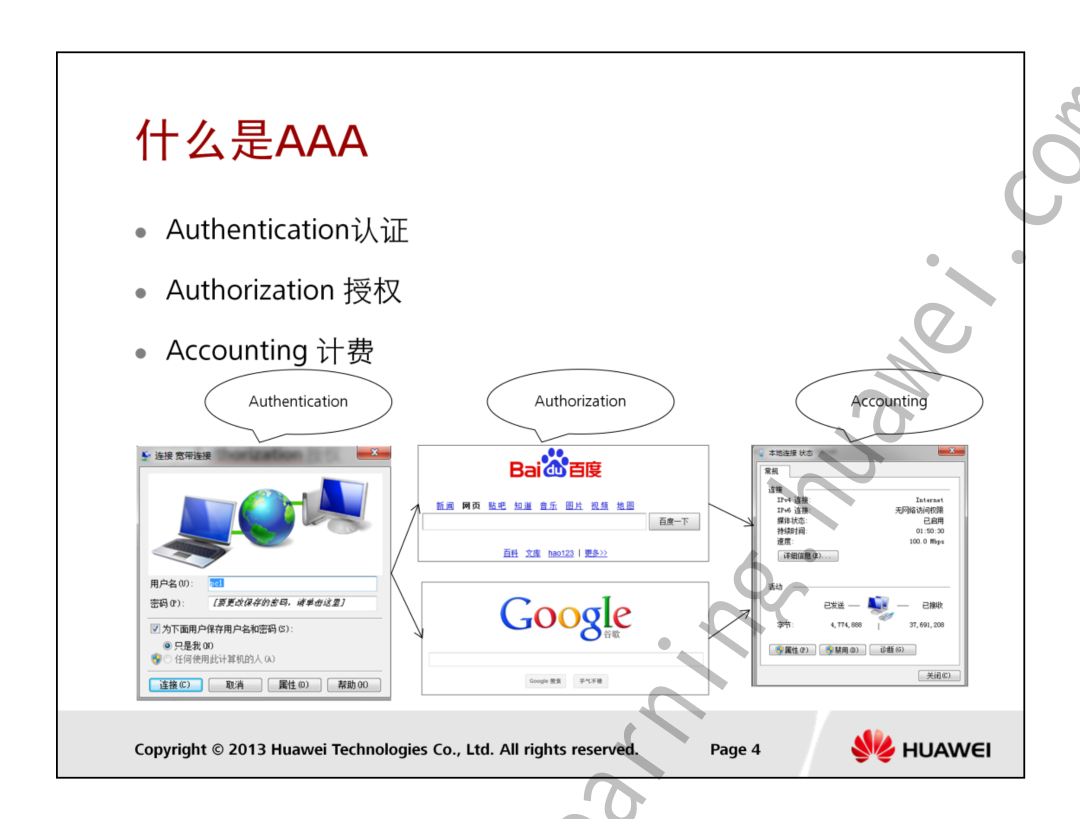


目录



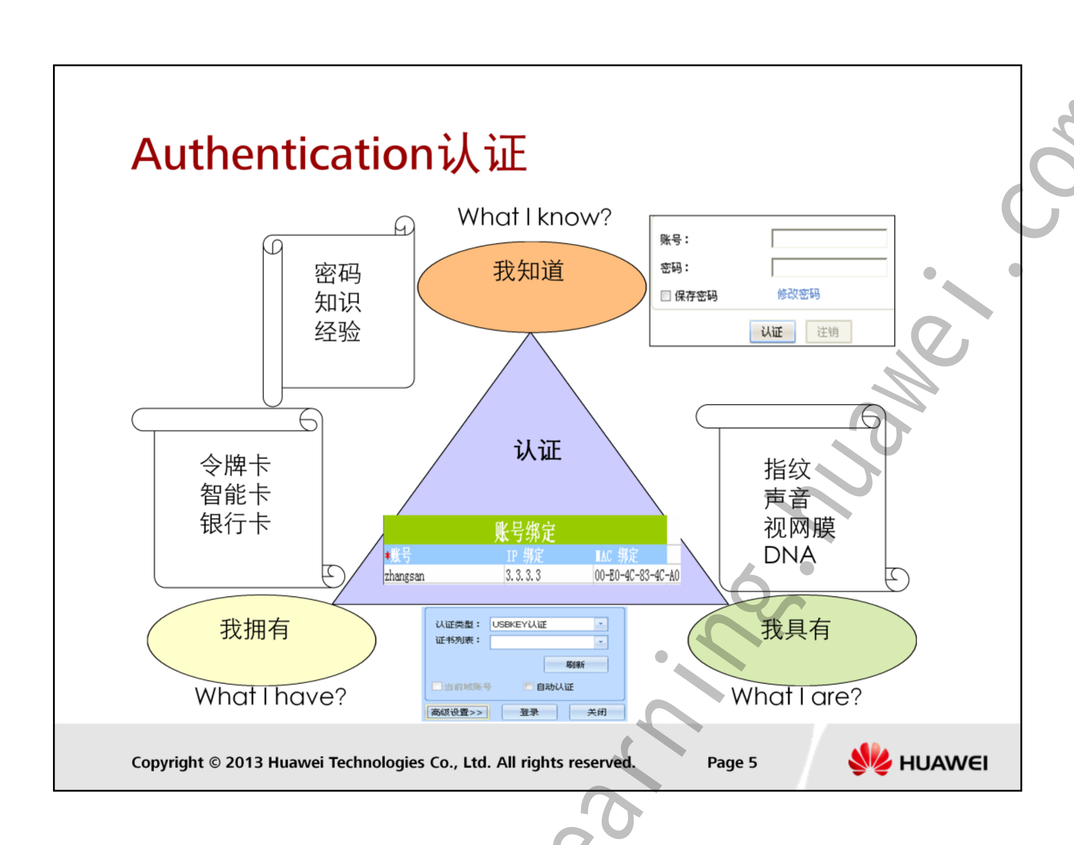


当前网络环境中，网络安全的威胁更多的来源于应用层，这也使得企业对于网络访问控制提出更高的要求。如何精确的识别出用户，保证用户的合法应用正常进行，阻断用户有安全隐患的应用等问题，已成为现阶段企业对网络安全关注的焦点。但IP不等于用户、端口不等于应用，传统防火墙基于IP/端口的五元组访问控制策略已不能有效的应对现阶段网络环境的巨大变化。

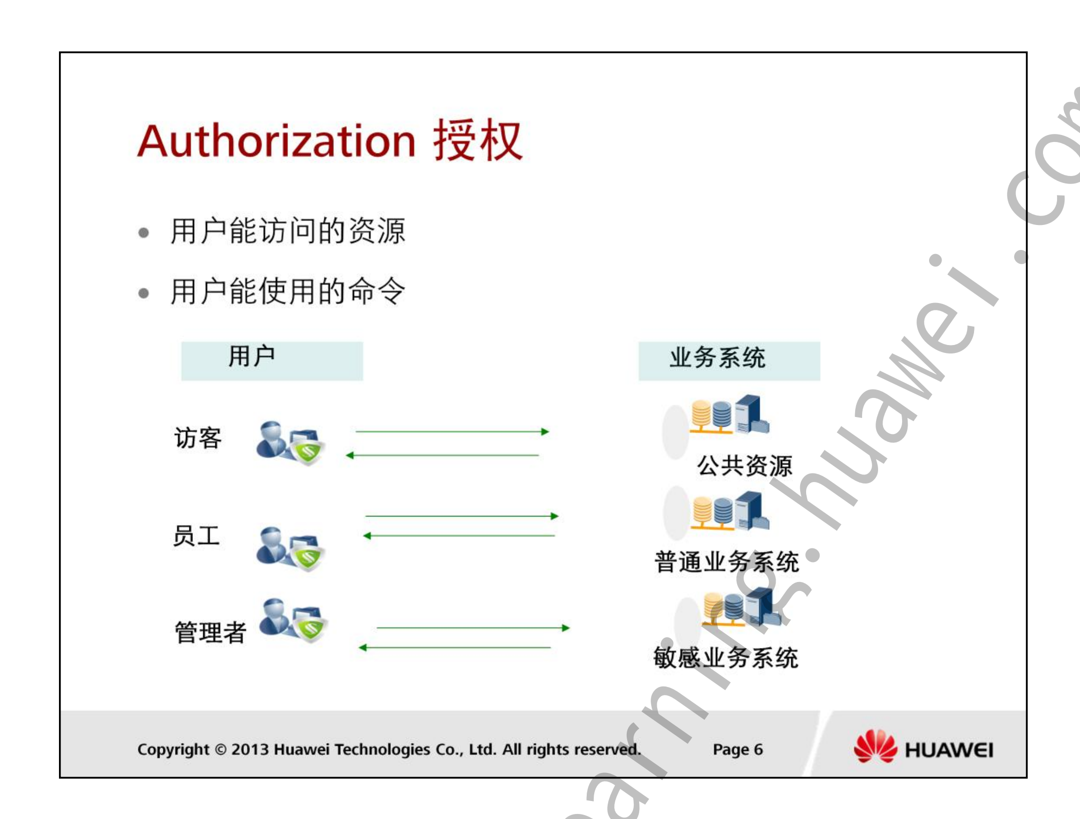


举例:

1. 当用户希望访问Internet访问资源。首先使用Authentication认证技术，用户输入用户名密码。
2. 当通过认证后，通过Authorization 授权，授权不同用户访问的资源，可以访问百度，或者Google。
3. 在客户访问期间，通过Accounting 计费，记录所做的操作和时长。



- 认证的方式包括：
  - 我知道：用户所知道的信息（如：密码、个人识别号（PIN）等）
  - 我拥有：用户所拥有的信息（如：令牌卡、智能卡或银行卡）
  - 我具有：用户所具有的生物特征（如：指纹、声音、视网膜、DNA）



授权用户可以使用哪些业务，公共业务，还是敏感业务。

授权用户管理设备，可以使用那些命令。如，可以是Display命令，不能是用delete，copy命令。

Accounting 计费

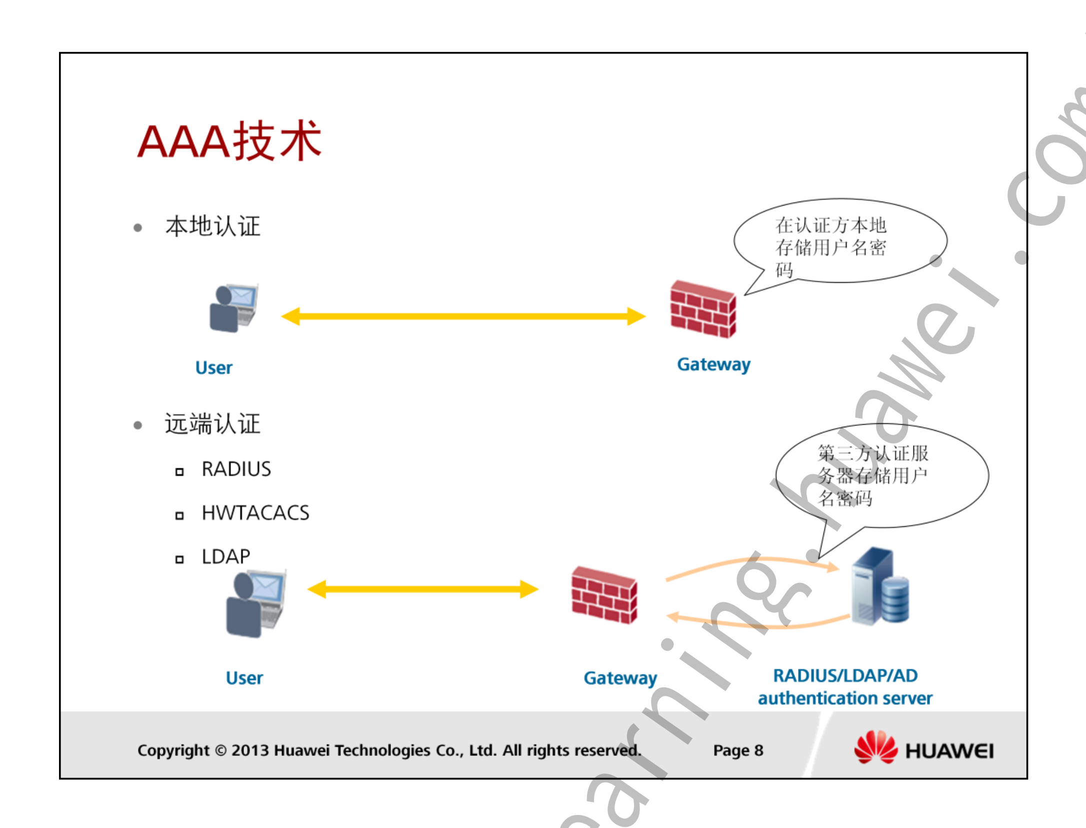
- 用户用多长时间
- 用户花了多少钱
- 用户做了哪些操作



 Page 7 HUAWEI

计费主要的含义有三个:

- 用户用多长时间
- 用户花了多少钱
- 用户做了哪些操作



- 不认证：

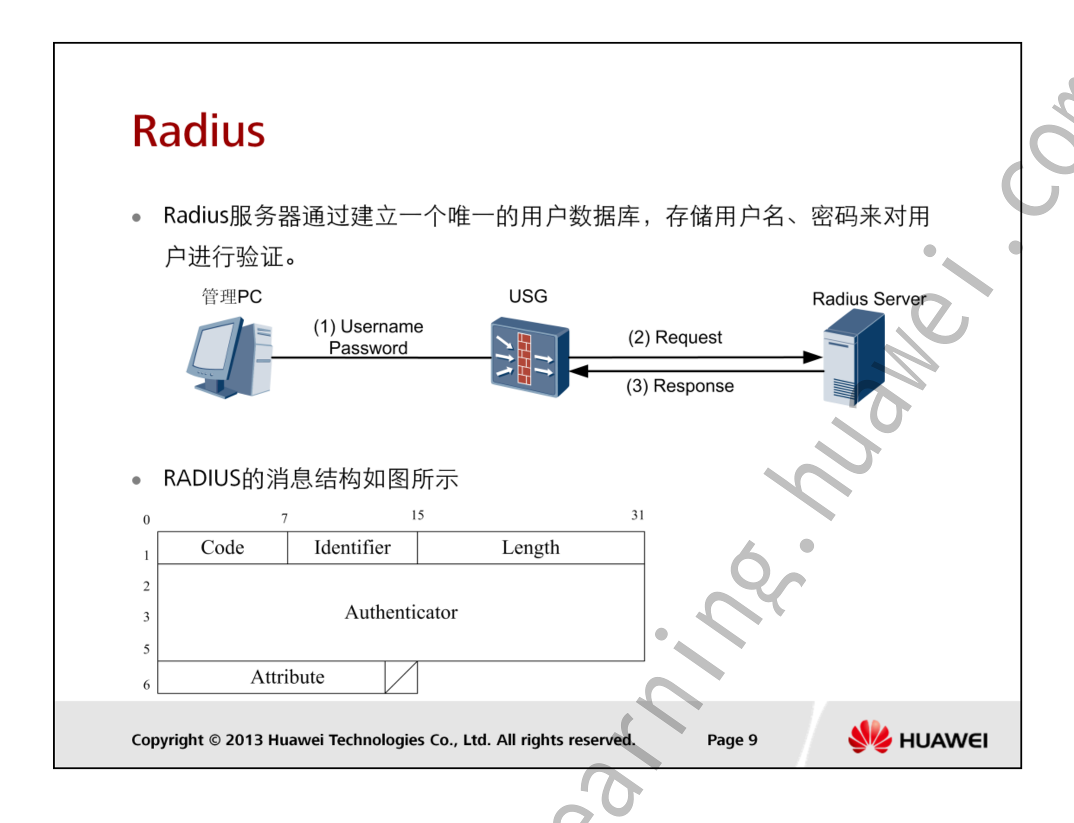
  对用户非常信任，不对其进行合法检查，一般情况下不采用这种方式。

- 本地认证：

  将用户信息（包括本地用户的用户名、密码和各种属性）配置在网络接入服务器上。本地认证的优点是速度快，可以为运营降低成本；缺点是存储信息量受设备硬件条件限制。

- 远端认证：

  将用户信息（包括本地用户的用户名、密码和各种属性）配置在认证服务器上。AAA支持通过RADIUS（Remote Authentication Dial In User Service）协议或HWTACACS （HuaWei Terminal Access Controller Access Control System）协议进行远端认证。

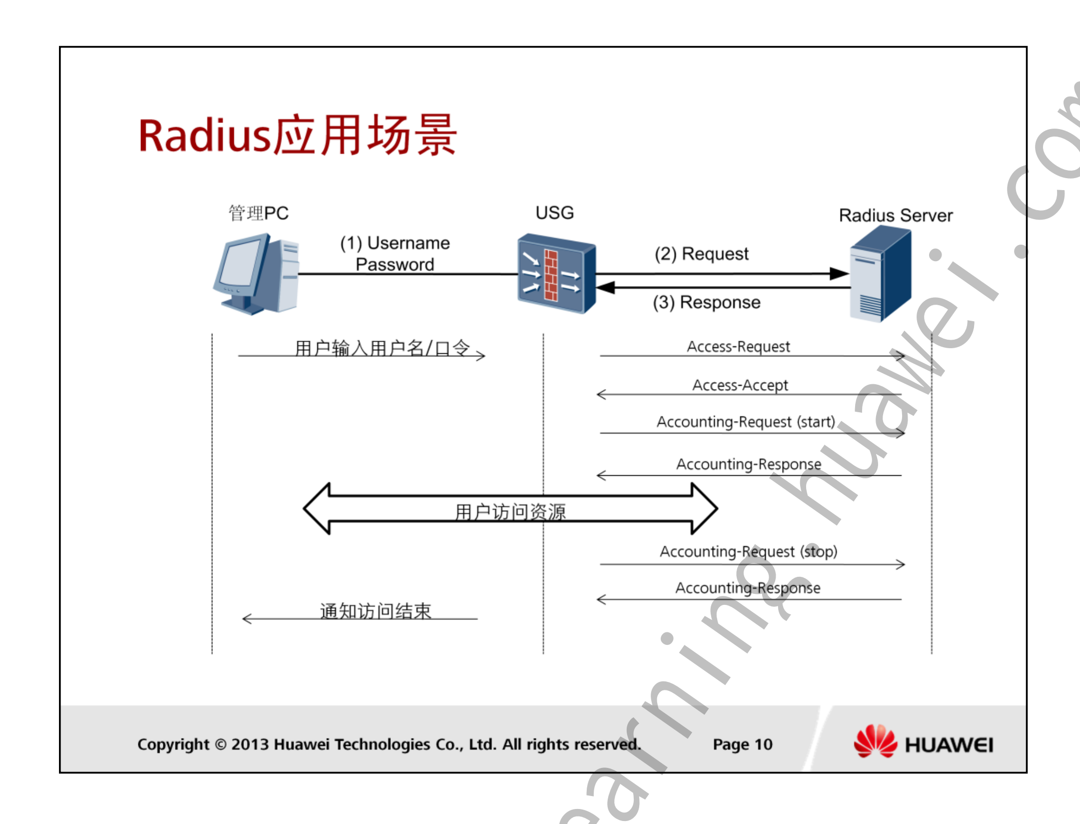


AAA可以用多种协议来实现，最常用的是RADIUS协议。RADIUS广泛应用于网络接入服务器NAS（Network Access Server）系统。NAS负责把用户的认证和计费信息传递给RADIUS服务器。RADIUS协议规定了NAS与RADIUS服务器之间如何传递用户信息和计费信息以及认证和计费结果，RADIUS服务器负责接收用户的连接请求，完成认证，并把结果返回给NAS。

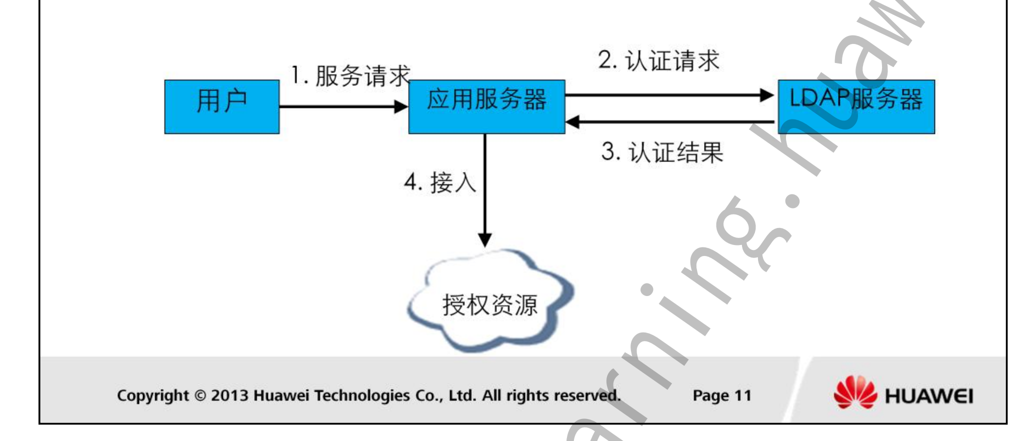
RADIUS使用UDP（User Datagram Protocol）作为传输协议，具有良好的实时性；同时也支持重传机制和备用服务器机制，从而具有较好的可靠性。

RADIUS客户端与服务器间的消息流程如下：

1. 用户登录USG或接入服务器等网络设备时，会将用户名和密码发送给该网络接入服务器；
2. 该网络设备中的RADIUS客户端（网络接入服务器）接收用户名和密码，并向RADIUS服务器发送认证请求；
3. RADIUS服务器接收到合法的请求后，完成认证，并把所需的用户授权信息返回给客户端；对于非法的请求，RADIUS服务器返回认证失败的信息给客户端。
   - Code：消息类型，如接入请求、接入允许等。
   - Identifier：一般是顺序递增的数字，请求报文和响应报文中该字段必须匹配。
   - Length：所有域的总长度。
   - Authenticator：验证字，用于验证RADIUS的合法性。
   - Attribute：消息的内容主体，主要是用户相关的各种属性。



- Radius报文交互流程
  - 用户输入用户名密码
  - 认证请求
  - 认证接受
  - 计费开始请求
  - 计费开始请求响应报文
  - 用户访问资源
  - 计费结束请求报文
  - 计费结束请求响应报文
  - 访问结束
- Code：包类型。包类型占1个字节，定义如下：
  - Access-Request——请求认证过程
  - Access-Accept——认证响应过程
  - Access-Reject——认证拒绝过程
  - Accounting-Request——请求计费过程
  - Accounting-Response——计费响应过程
  - Access-Challenge ——访问质询



LDAP也是基于C/S架构的，LDAP服务器负责对来自应用服务器的请求进行认证，同时还指定用户登录的应用服务器所允许访问的资源范围等。

HWTACACS

- HWTACACS是在TACACS基础上进行了功能增强的一种安全协议，主要用于接入用户的认证、授权和计费。
- HWTACACS协议与RADIUS协议的比较

	HWTACACS	RADIUS
端口使用	使用TCP协议，网络传输更可靠	使用UDP协议。认证和授权端口号是1812和1813，或者1645和1646.
加密情况	除了标准的HWTACACS报文头，对报文主体全部进行加密	只是对认证报文中的密码字段进行加密
认证和授权	认证与授权分离	认证与授权一起处理
应用	适于进行安全控制	适于进行计费
配置命令授权	支持对配置命令进行授权	不支持对配置命令进行授权

 Page 12



HWTACACS是在TACACS基础上进行了功能增强的一种安全协议，主要用于接入用户的认证、授权和计费。

用户认证分类

- AAA技术为用户认证提供手段。
- 用户认证分类有：
  - 免认证
  - 密码认证
  - 单点登录(仅在上网用户中体现)

Page 13

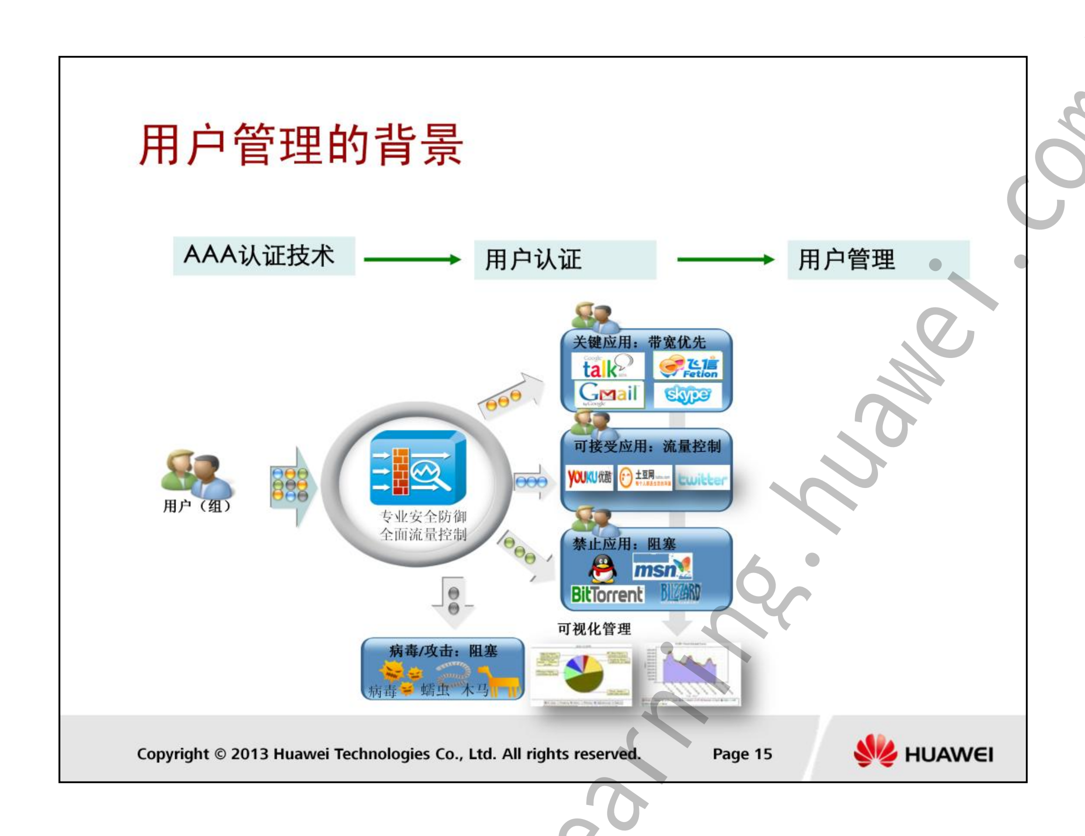


- 免认证
  - VIP
  - 临时访客
- 密码认证：
  - 对于普通的公司员工，一般采用密码认证，认证形式方便快捷。支持设备与LDAP，Radius，AD多种认证。
- 单点登录(仅在上网用户中体现)
  - 如果当前网络中已经部署了AD服务器身份认证系统，则设备可以通过单点登录功能，使得设备与AD服务器联动，识别出已在AD服务器上认证通过的用户，从而避免用户上网时再次要求输入用户名/密码，设备对用户的认证过程透明。



目录





Page 15
HUAWEI

用户管理将分为不同的用户组，通过对用户认证，将用户打上标签，并且为用户组赋予不同的权限和应用，从而实现安全的目标。

举例：

将公司员工（用户）加入用户组，然后针对用户或用户组进行网络行为控制和审计，根据用户或用户组进行策略的可视化制定，提高策略制定的易用性，报表中体现用户信息，对用户进行上网行为分析，以达到对用户（而非单纯的IP地址）行为的追踪审计，解决现网应用中同一用户对应IP经常变化带来的应用行为策略控制难题。

用户管理分类

- 上网用户管理 
  - “上网用户”指通过USG设备访问资源的用户，包括内网主动发起上网行为的对象，如内网PC。
- 接入用户管理 
  - “接入用户”指PPP或隧道建立过程中使用的用户。USG对这些用户提供本地认证、RADIUS认证、HWTACACS认证，可验证用户身份的合法性并为合法用户进行授权，防止非法用户进行访问。
- 管理员用户
  - “管理员用户”指通过Telnet、SSH、web、FTP等协议或通过Console接口访问设备并对设备进行配置或操作的用户。

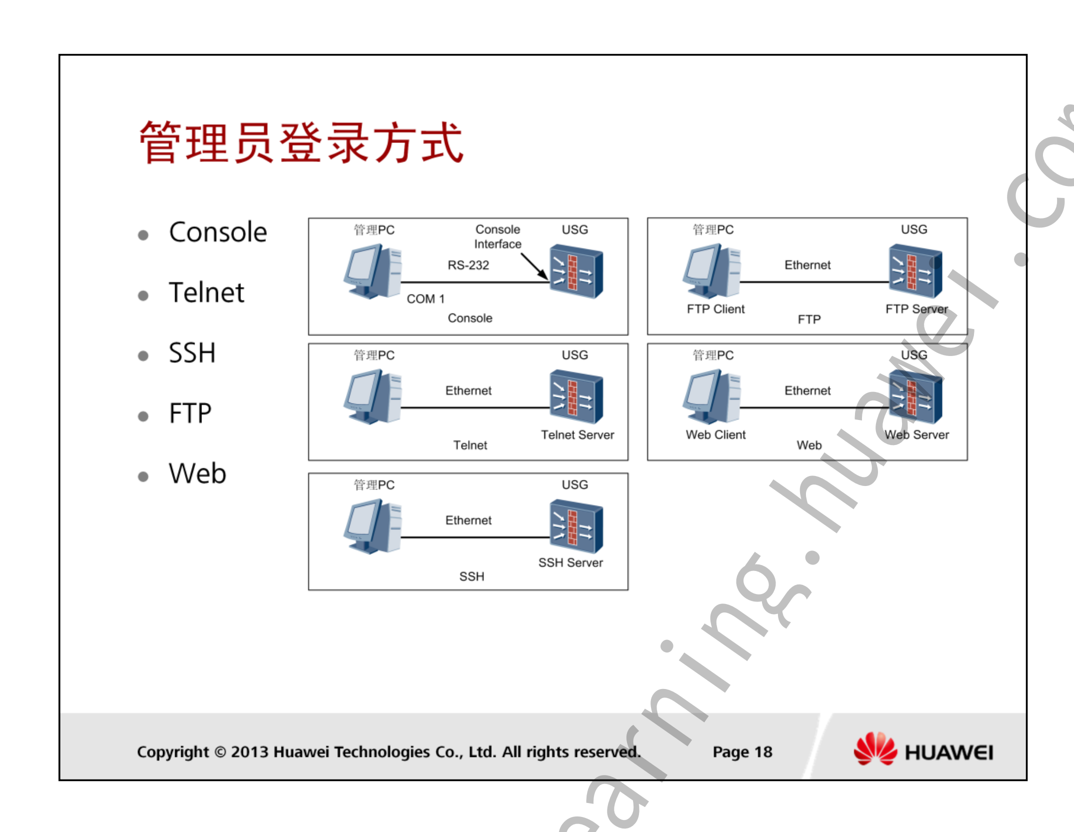
 Page 16 

- 管理员用户：管理员主要为了实现对设备的管理、配置和维护，登录方式可以分为：
  - Console
  - Web
  - Telnet
  - FTP
  - SSH
- 接入用户主要为了实现访问网络，
  - 802.1X接入用户
  - PPP接入用户
  - SSL接入用户
- 上网用户
  - 上网用户是网络访问的标识主体，是设备进行网络权限管理的基本单元。设备通过对访问网络的用户进行身份认证，从而获取用户身份，并针对用户的身份进行相应的策略控制。



目录





管理员主要为了实现对设备的管理、配置和维护，登录方式可以分为：

- Console
  - Console接口提供命令行方式对设备进行管理，通常用于：
  - 设备的第一次配置。或者设备配置文件丢失，没有任何配置。
  - 当设备系统无法启动时，可通过Console口进行诊断或进入BootRom进行升级。
- Web
  - 终端通过HTTP/HTTPS方式登录到设备进行远程配置和管理。
- Telnet
  - Telnet是一种传统的登录方式，通常用于通过命令行方式对设备进行配置和管理。
- FTP
  - FTP管理员主要对设备存储空间里的文件进行上传和下载。
- SSH
  - SSH提供安全的信息保障和强大的认证功能，在不安全的网络上提供一个安全的“通道”。此时，设备作为SSH服务器。

Console/telnet/Ftp设备管理类型

- 新建管理员Client01，并设置设备管理类型Console, Telnet, FTP。

系统 > 管理员 > 管理员

新建管理员

用户名 client001 *

密码 ********* *(1-16个字符)

确认密码 ********* *

用户级别 管理级

信任主机 #1

高级

应用 返回

设置信任主机IP，指定特定的主机访问

用户级别设置为管理级别，不仅可以配置设备，而且可以管理文件系统，用于软件升级。

- Notes: 默认Console, telnet, ftp配置，无需要另外配置。

 Page 19



步骤1: User-interface

- Console:

  [sysname] user-interface console 0

  [sysname-ui-con0] authentication-mode aaa

- Telnet:

  [sysname] user-interface vty 0 3

  [sysname-ui-vty0] authentication-mode aaa

  [sysname-ui-vty0] protocol inbound all

步骤2: AAA View

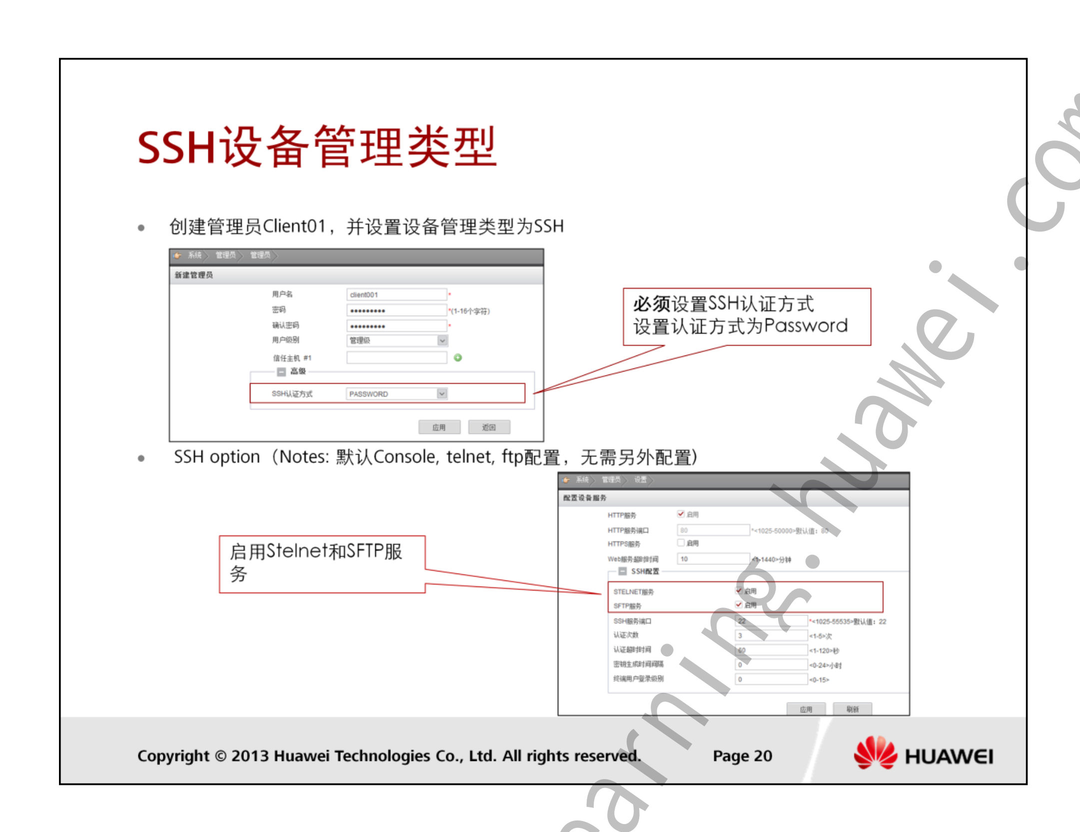
  [USG] aaa

  [USG-aaa] local-user client001 password cipher Admin@123

  [USG-aaa] local-user user-name service-type telnet terminal ftp

  [USG-aaa] local-user client001 level 3

  [USG-aaa] local-user admin ftp-directory flash:



- 配置RSA本地密钥对。

<USG> system-view

[USG] rsa local-key-pair create

It will take a few minutes. Input the bits in the modulus[default = 512]:512

Generating keys... ..++++++++++++ ....

- 配置VTY用户界面。

[USG] user-interface vty 0 4

[USG-ui-vty0-4] authentication-mode aaa

[USG-ui-vty0-4] protocol inbound ssh

  - 新建用户名为Client001的SSH用户，且认证方式为password。

[USG] ssh user client001

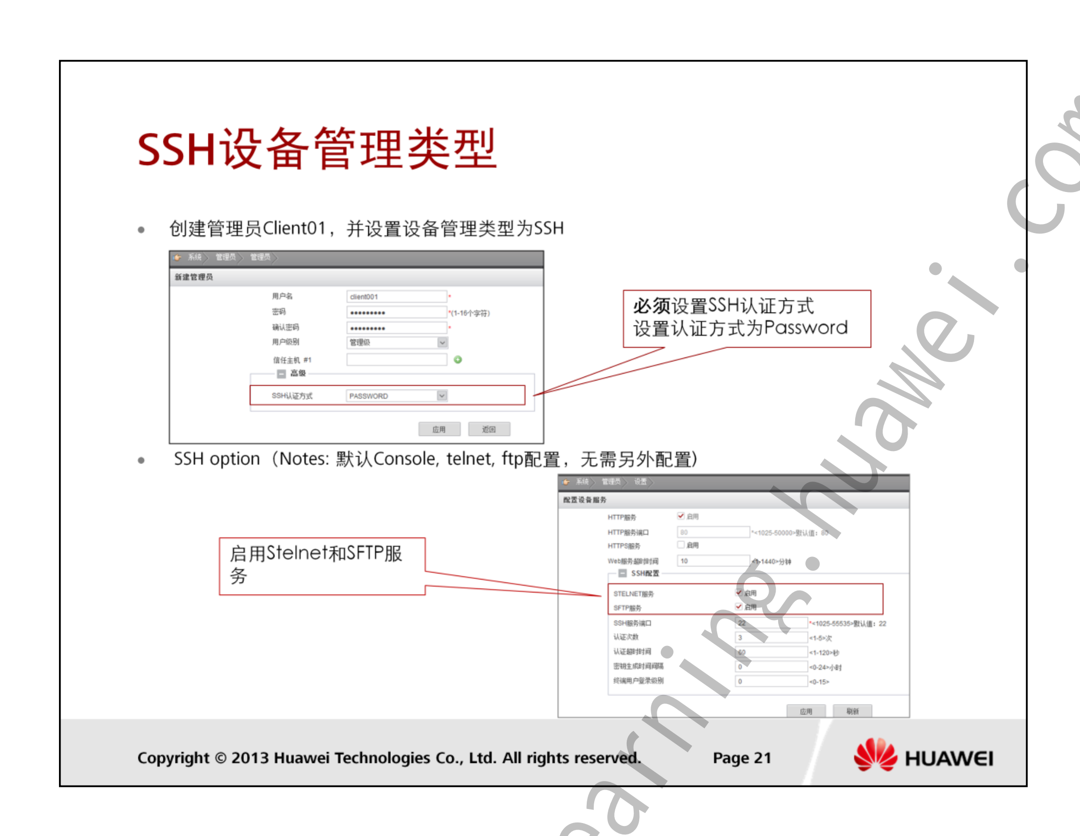
[USG] ssh user client001 authentication-type password

- 为SSH用户Client001配置密码为Admin@123。

[USG] aaa

[USG-aaa] local-user client001 password cipher Admin@123

[USG-aaa] local-user client001 service-type ssh

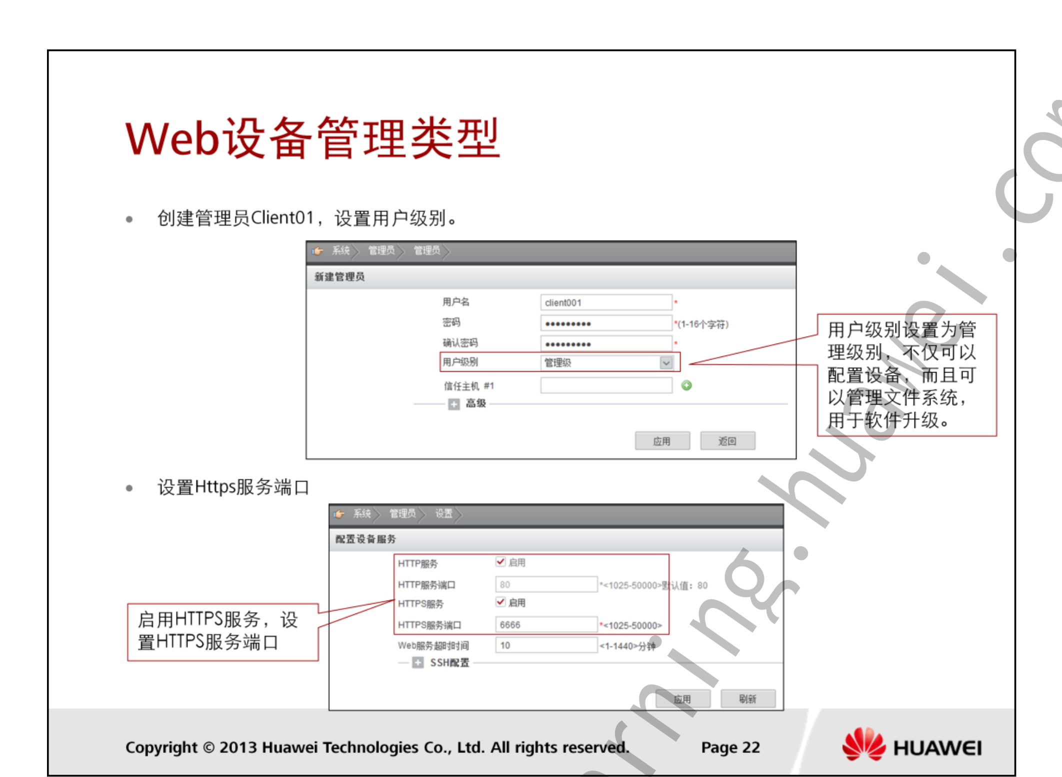


- 配置SSH用户Client001的服务方式为STelnet，并启用STelnet服务。

  [USG] ssh user client001 service-type stelnet

  [USG] stelnet server enable

  以上配置完成后，运行支持SSH的客户端软件，建立SSH连接



- 启动Web管理功能。

  [USG] web-manager security enable port 6666

- 配置Web用户。

  [USG] aaa

  [USG-aaa] local-user webuser password cipher Admin@123

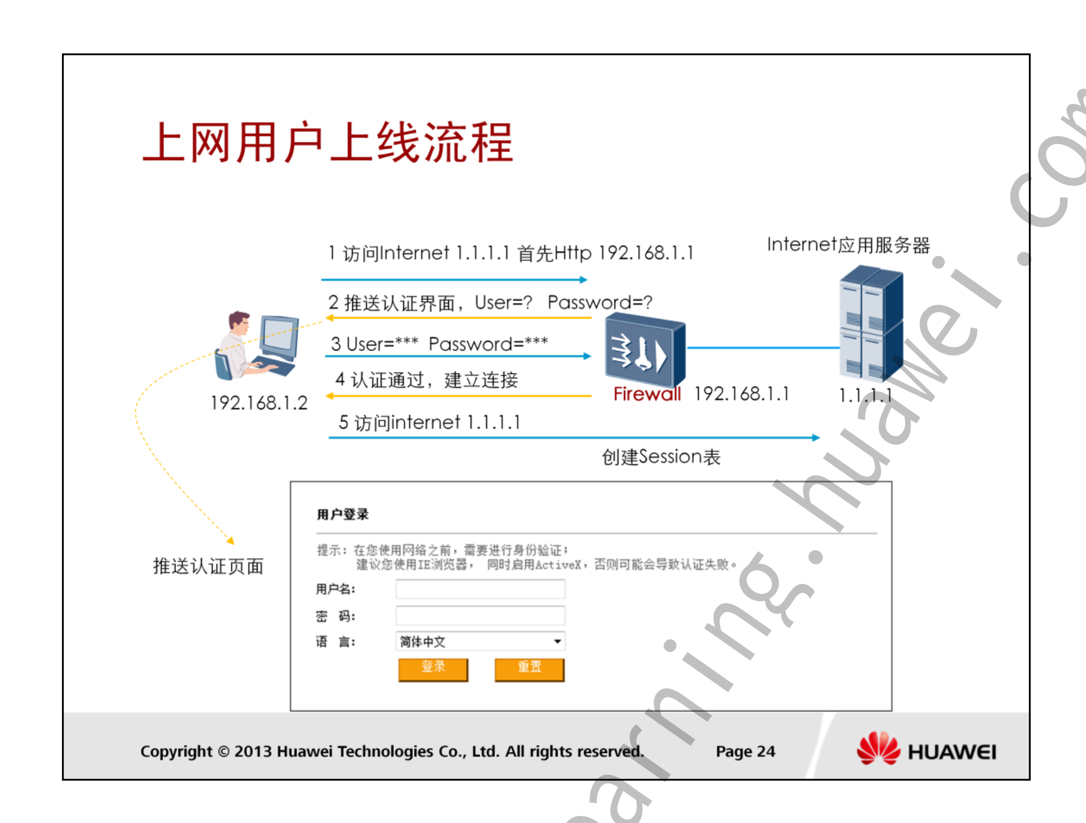
  [USG-aaa] local-user webuser service-type web

  [USG-aaa] local-user webuser level 3



目录





上网用户上线的流程如下：

1. 访问Internet 1.1.1.1 首先Http 192.168.1.1
2. 推送认证界面，User=? Password=?
3. User=*** Password=***
4. 认证通过，建立连接
5. 访问internet 1.1.1.1，设备创建Session表

组织结构管理

- 系统默认有一个根用户组
- 每个用户组可以包括多个用户和用户组
- 每个用户组只能属于一个父用户组；
- 每个用户至少属于一个用户组，也可以属于多个用户组；

User	Sub Group	Sub Group	Default Group
sunxing		development	root
zhansan	firewall		
Leader-svn	SVN		
	Leader		

root
development
sunxing
firewall
svn
leader
zhansan
leader-svn

 Page 25 HUAWEI

为了给不同的用户或部门进行差异化管理，分配不同的权限，需要对组织结构进行规划和管理。防火墙支持创建树型的组织结构，这种结构和通常的行政架构比较类似，非常方便规划和管理。

系统默认有一个根用户组，其余所有用户组都是根用户组的子组，或者子组的子组；

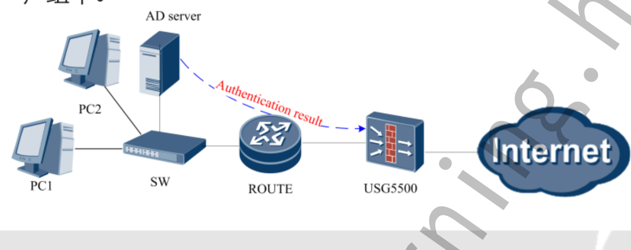
每个用户组可以包括多个用户和用户组，但每个用户组只能属于一个父用户组；

每个用户至少属于一个用户组，也可以属于多个用户组；

每个用户（组）可以被安全策略、限流策略、等引用，从而实现基于用户的权限和带宽资源控制。

单点登录

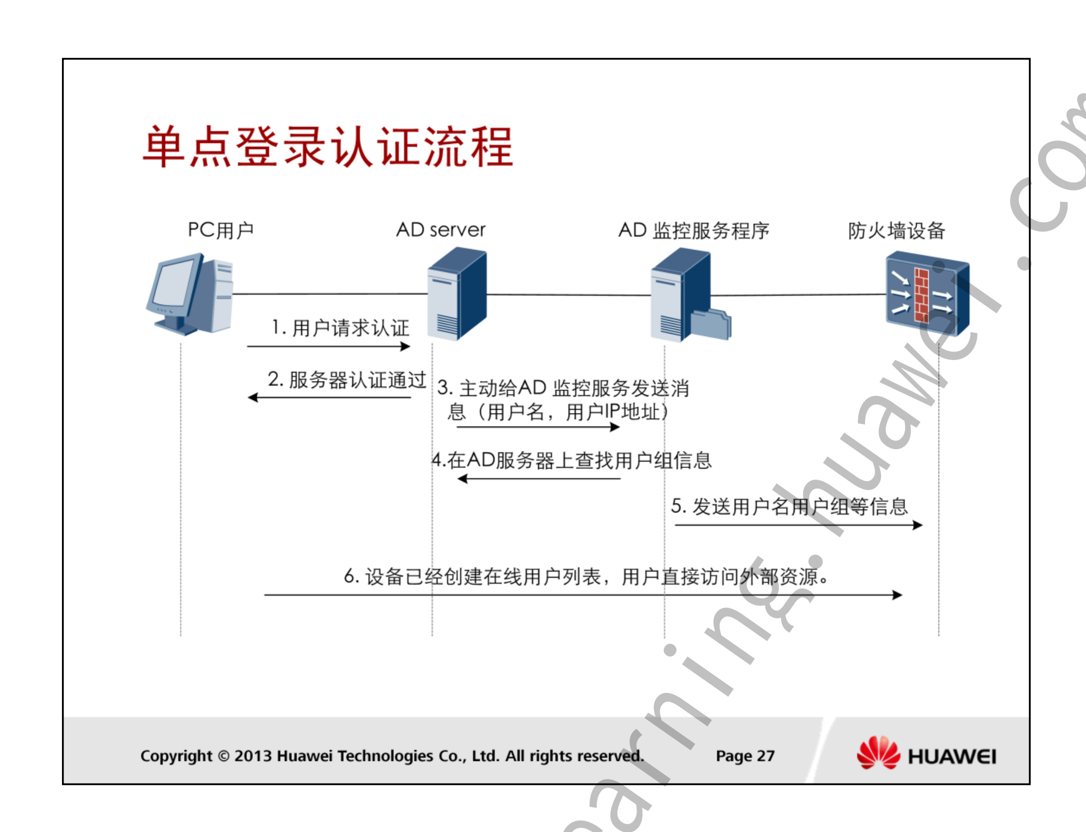
- 用户和AD认证服务器组网需求为:
  - 用户管理需求
    - 希望防火墙可以识别出经过AD域账号认证通过的用户，避免用户上网时再次要求输入用户名/密码。
    - 员工登录成功后, 自动将其用户信息导入到本地, 且添加到指定的用户组中。



 Page 26 HUAWEI

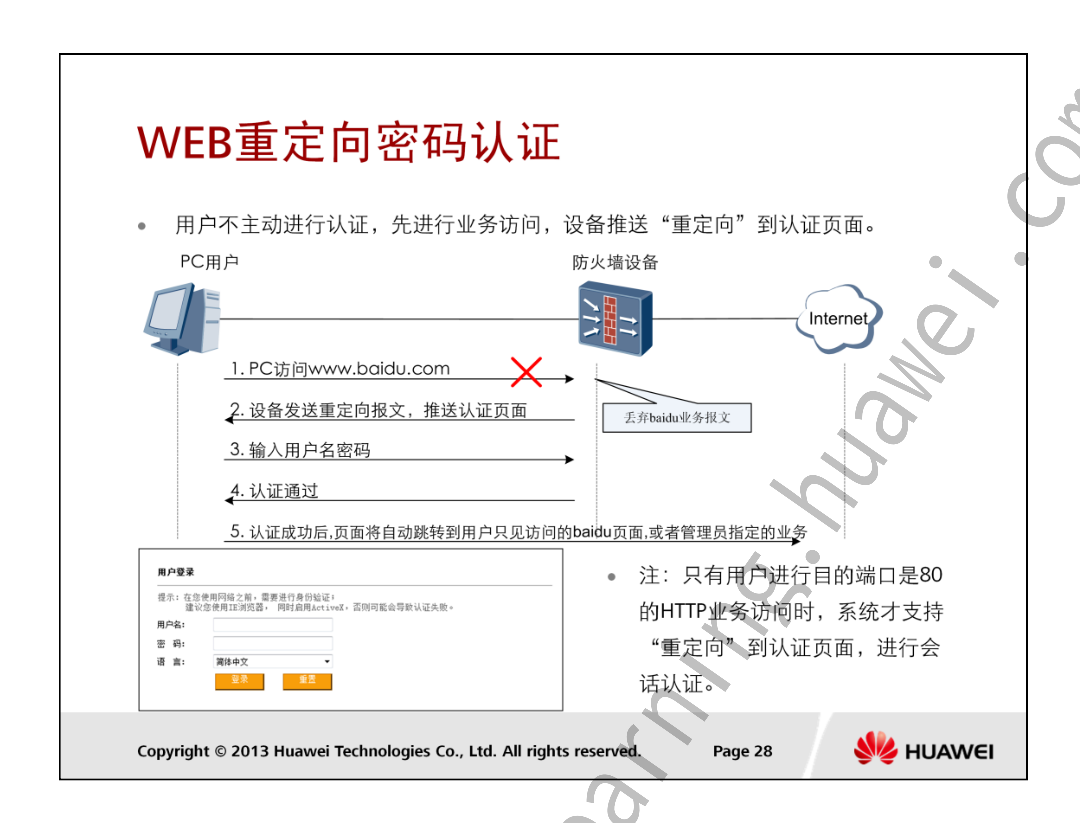


设备通过启用单点登录功能，可以识别出经过这些身份认证系统认证通过的用户，避免用户上网时再次要求输入用户名/密码。



用户直接向AD服务器认证,设备不干涉用户认证过程;

- AD监控服务处理:
  - 客户端认证成功后，主动给AD 监控服务发送用户认证成功消息，AD监控服务从该消息中获取对应的用户名和IP地址信息;
  - AD监控服务使用获取的用户在AD服务器上查找用户的组信息;
  - AD监控服务将获取到用户名、用户组名、用户IP发送到设备（支持丢包重传机制）；
- 设备侧处理:
  - 接收并解析AD服务器发送过来的报文;
  - 根据收到的用户登录信息创建在线用户监控表项;



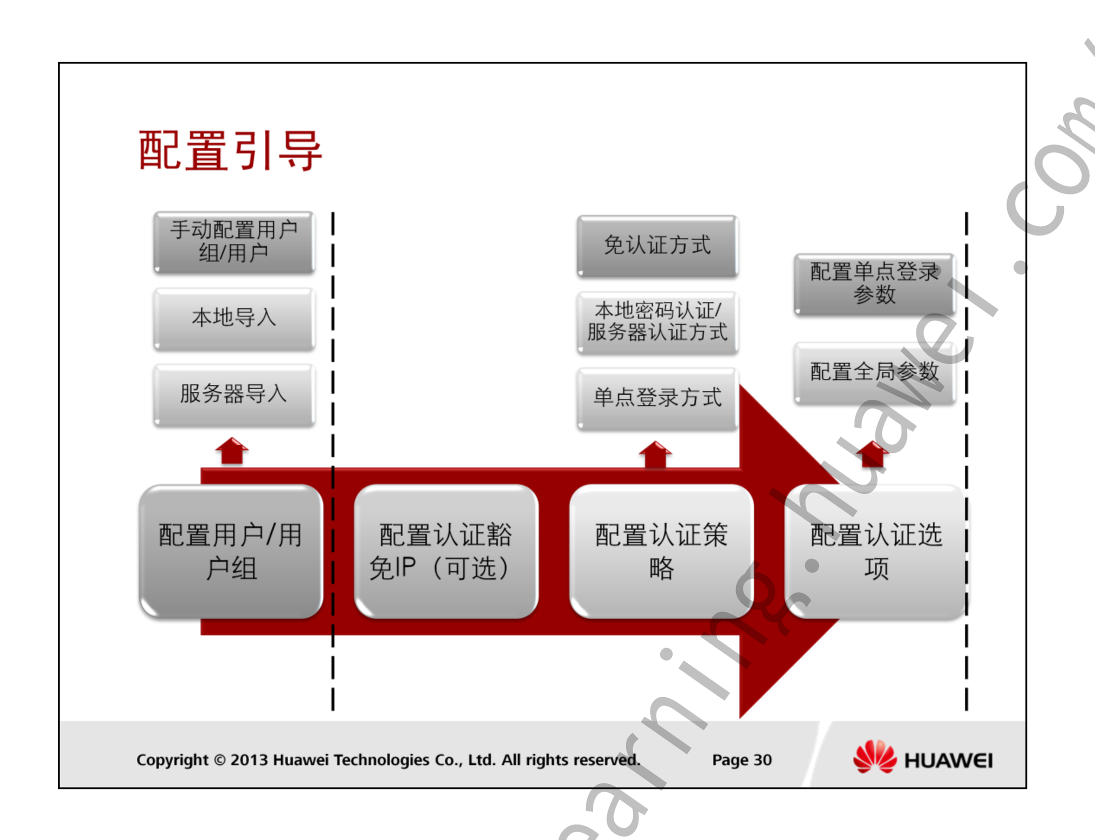
Web重定向密码认证处理过程:

1. PC访问www.baidu.com
2. 设备收到用户访问baidu的业务报文后, 将该报文丢弃, 然后构造HTTP重定向报文回应用户, 将页面重定向至”设备认证页面”
3. 用户输入用户名,密码信息进行认证;
4. 认证成功后,页面将自动跳转到用户只见访问的baidu页面,或者管理员指定的业务(管理员可配)。

上网用户认证

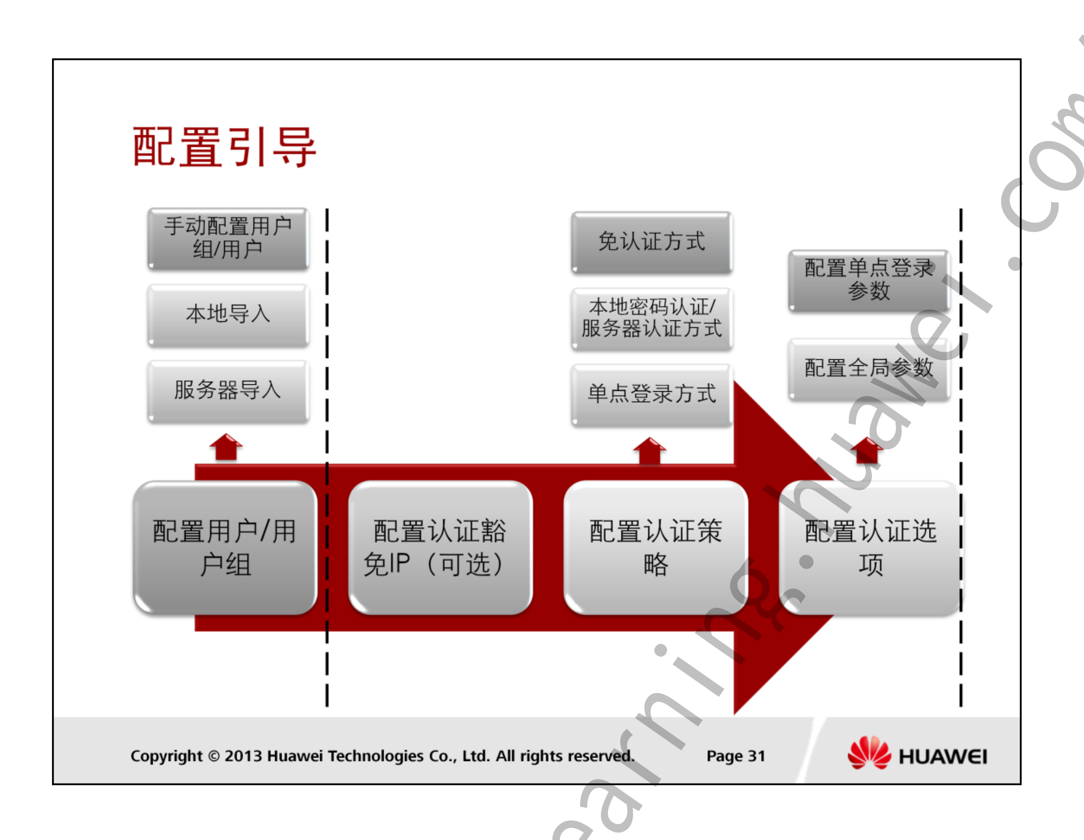
- 配置引导
- 典型配置举例-免认证
- 典型配置举例-密码认证
- 典型配置举例-单点登录





配置组/用户：设备实施基于用户/用户组的管理之前，必须先创建用户/用户组。设备支持管理员手动配置、本地导入和服务器导入多种创建方式。

- 手动配置组/用户
  - 缺省情况下，设备默认自带根用户组root组。
  - 当需要根据企业组织结构创建用户组时，并基于用户组进行网络权限分配等管理时，该步骤必选。
  - 当对用户进行本地密码认证时，必须要在本地创建用户，并配置本地密码信息。
- 本地导入
  - 本地导入支持将CSV格式文件和数据库dbm文件的用户信息导入到设备本地。
- 服务器导入
  - 网络中，使用第三方认证服务器的情况非常多，很多公司的网络都存在认证服务器，认证服务器上存放着所有用户和用户组信息。从认证服务器上批量导入用户是指通过服务器导入策略，将认证服务器上用户（组）信息导入到设备上。



配置用户认证：管理员通过配置认证策略和认证选项，指定某一个或几个IP地址范围内的用户发起的HTTP报文经过设备时，采用哪种认证方式进行身份认证。

- 配置认证豁免IP　当要定义不参与用户管理的IP地址范围时，必选。
- 配置认证策略　　设备基于用户的源IP地址对用户进行认证前，必须先创建基于IP地址范围的用户认证策略。
- 配置单点登录参数 当认证策略中只允许单点登录时，必选。
- 配置全局参数　　认证全局参数已有缺省配置。

创建用户和用户组



- 组/用户
  - 设备实施基于用户/用户组的管理之前，该用户/用户组必须在设备上存在。通过组/用户节点，在设备上手动创建用户/用户组。
- 新建用户组

root组是设备默认自带的根用户组，不能删除，也无需创建。root组的组名不能修改，但可以配置其描述信息，方便识别。

所有创建的用户组都是root组的子组，或者子组的子组。

  - 选择“用户 > 上网用户 > 组/用户”。
  - 可选：在“组织结构”中选择需要添加子组的用户组。
  - 窍门：新建前，如果预先选定所属的用户组，则设备会自动将该用户组指定为所属组。
  - 在“成员管理”中单击“新建”，选择“新建组”。
- 新建单个用户

新建单个用户是指同一时刻只能创建一个用户。与新建多个用户不同的是，新建单个用户时，除能完成新建多个用户涉及的配置项外，还能配置用户显示名、IP/MAC地址双向绑定。

  - 选择“用户 > 上网用户 > 组/用户”。

配置用户属性

用户的账号过期时间

允许该登录名同时在多台计算机上登录

如果该用户是MAC地址双向绑定免认证用户，当用户和设备之间存在三层设备时，则该用户将登录失败；
如果该用户是MAC地址绑定用户，但采用了单点登录方式进行认证，此时，MAC地址绑定属性不生效。

 Page 33 HUAWEI

- 账号过期时间
  - 用户的账号过期时间。
- 允许多人同时使用该账号登录
  - 选中该参数，表示允许多人同时使用该用户的登录名登录，即允许该登录名同时在多台计算机上登录。
  - 去选中该参数，表示同一时刻仅允许该登录名在一台计算机上登录。
- IP/MAC绑定方式
  - 用户与IP/MAC地址的绑定方式。
    - 选中“单向绑定”，表示用户只能使用指定的IP/MAC地址进行认证，但同时允许其他用户也使用该IP/MAC地址进行认证。
    - 选中“双向绑定”，表示用户只能使用指定的IP/MAC地址进行认证，并且指定的IP/MAC地址仅供该用户使用。当一个IP/MAC地址被双向绑定后，其他单向绑定此IP/MAC地址的用户将无法登录。
- IP/MAC地址
  - 与用户绑定的IP地址、MAC地址或IP/MAC地址对。

配置认证策略-免认证

用户 > 上网用户 > 认证策略

认证策略列表

新建 删除 刷新 清除全部命中次数

策略名称	IP地址范围	认证方式	新用户认证选项	命中次数	启用	配置
guest	192.168.0.0-192.168.0.100	免认证	临时用户	0		

第 1 页共 1 页　显示 1 - 1，共 1 条

用户 > 上网用户 > 认证策略

新建认证策略

名称：guest

描述：

IP地址范围1：192.168.0.0-192.168.0.100

认证方式：本地密码认证/服务器认证（本地密码认证/服务器认证、免认证、只允许单点登录）

认证服务器类型

认证服务器名称

新用户认证选项（新用户指本地不存在的账户）

应用　返回

免认证：表示用户不需要进行基于Web的用户名密码认证。
如果设备同时启用了单点登录，则优先通过单点登录功能对用户进行认证。

　Page 34　HUAWEI

- 免认证

表示用户不需要进行基于Web的用户名密码认证。如果设备同时启用了单点登录，则优先通过单点登录功能对用户进行认证。在没有单点登录或者单点登录不成功的情况下，设备根据数据包的源IP地址、源MAC地址来识别用户。

配置认证策略-密码认证

- 选择用户>上网用户>认证策略
  - 设置认证策略的认证服务器类型为RADIUS
- 选择用户>认证服务器>RADIUS服务器
  - 设置RADIUS认证参数

选择认证服务器类型RADIUS

设置RADIUS共享密钥，密钥和RADIUS服务器一致

 Page 35 HUAWEI

密码认证：表示用户需要进行基于Web的用户名密码认证，包括本地密码认证和服务器认证。

- 如果设备同时启用了单点登录，则优先通过单点登录功能对用户进行认证。
- 在没有单点登录或者单点登录不成功的情况下，设备在本地查找用户：
  - 如果用户在本地存在且已配置本地密码，则进行本地密码认证。
  - 如果用户在本地不存在，或者在本地存在但是没有配置本地密码，则向认证服务器认证。

配置认证策略-密码认证

用户 > 上网用户 > 认证策略

认证策略列表

新建 删除 刷新 清除全部命中次数

策略名称	IP地址范围	认证方式	新用户认证选项	命中次数	启用	配置
guest	192.168.0.0-192.168.0.100	免认证	临时用户	1	☑	
employ	192.168.1.1-192.168.1.100	本地密码认证/服务器认证	添加到组	0	☑	

LDAP认证

选择认证参数

AD认证

选择认证参数

- 设置认证策略的认证服务器类型LDAP或者AD
- 设置AD或LDAP认证参数

HUAWEI

在Web配置界面中，配置密码认证的步骤为:

1. 选择用户>上网用户>认证策略
   - 设置认证策略的认证服务器类型为LDAP或者AD
2. 选择用户>认证服务器>LDAP或者AD服务器
   - 设置LDAP或者AD认证参数

配置认证策略-单点登录

用户 > 上网用户 > 认证策略

认证策略列表

新建 删除 刷新 清除全部命中次数

策略名称	IP地址范围	认证方式	新用户认证选项
guest	192.168.0.0-192.168.0.100	免认证	临时用户
employ	192.168.1.1-192.168.1.100	本地密码认证/服务器认证	添加到组
hr	192.168.2.1-192.168.2.100	只允许单点登录	添加到组

用户 > 上网用户 > 认证策略

新建认证策略

名称 HR

描述

IP地址范围1 192.168.2.1-192.168.2.100

认证方式 只允许单点登录

新用户认证选项（新用户指本地不存在的账户）

应用 返回

新建认证策略

设置接入用户的IP地址

选择认证方式为单点登录

只允许单点登录：表示只允许用户通过单点登录方式进行认证。



在Web配置界面中，配置Web重典型密码认证的步骤为：

1. 选择“用户 > 上网用户 > 认证选项”。
2. 选择“全局配置”页签。
   - 跳转到最近使用的Web页面
     - 认证方式为密码认证的用户认证通过后的跳转页面为最近使用的Web页面，即用户认证通过后，Web页面跳转到用户认证前请求的页面。
   - 跳转到自定义URL页面
     - 针对密码认证用户，用户认证通过后的跳转页面为自定义URL页面。针对免认证用户，当用户上线后第一次访问HTTP（80端口）业务时，系统将给用户推送该URL页面。
     - 以“http://”或“https://”开头，例如http://www.test.com。
   - 认证端口
     - 用户管理Web认证端口。
     - 当设备正在处理业务时，修改Web认证端口将可能影响用户业务



CSV支持登录名、显示名、所属组、描述信息、密码、IP/MAC绑定信息、绑定模式、帐号状态、有效期信息

DBM导出是从Ramdisk导出用户数据库文件到指定目录

用户导入是指批量导入用户信息到设备，支持本地导入和服务器导入。其中，本地导入支持CSV格式文件；服务器导入支持LDAP服务器和AD服务器导入。

- 从CSV格式文件中批量导入用户
  - CSV格式文件导入是指：将用户信息（登录名、显示名、所属组路径、用户描述、本地密码等）按照指定格式的CSV表格文件预先编辑完成，再将CSV格式文件中的用户信息导入到设备内存中。
  - 将之前从设备上导出的CSV格式文件中的用户信息导入到设备内存中。
    - 选择"用户 > 上网用户 > 用户导入"。
    - 选择"本地导入"页签。
- 从认证服务器上批量导入用户
  - 网络中，使用第三方认证服务器的情况非常多，很多公司的网络都存在认证服务器，认证服务器上存放着所有用户和用户组信息。从认证服务器上批量导入用户是指通过服务器导入策略，将认证服务器上用户（组）信息导入到设备上。

通过本地和服务器导入用户

- 选择“用户 > 上网用户 > 用户导入”。
- 本地导入
  - 本地导入支持将CSV格式文件和数据库dbm文件的用户信息导入到设备本地。
- 服务器导入
  - 从认证服务器上批量导入用户是指通过服务器导入策略，将认证服务器上用户（组）信息导入到设备上。

成员管理

新建 删除 刷新 批量修改 移动 导出 导入 请输入名称 查询 高级查询

名称 所属组 绑定信息 账号过期时间 描述

用户导入

CSV格式文件导入

从文件中导入用户（指定格式的CSV表格文件） CSV模板

浏览...

自动创建用户组

当前用户存在时，覆盖本地用户记录

开始导入

下载CSV模板，补充完整数据后，点击浏览，并上传数据。

 Page 40 HUAWEI

- 设备只支持从AD和LDAP服务器批量导入用户。
  - 选择“用户 > 上网用户 > 用户导入”。
  - 选择“服务器导入”页签。

在线用户管理

- 若需要限制某些用户在某段时间内所有上网行为，可以冻结指定的在线用户。
- 若管理员觉察到某些用户不可信，可以强制注销指定的在线用户。



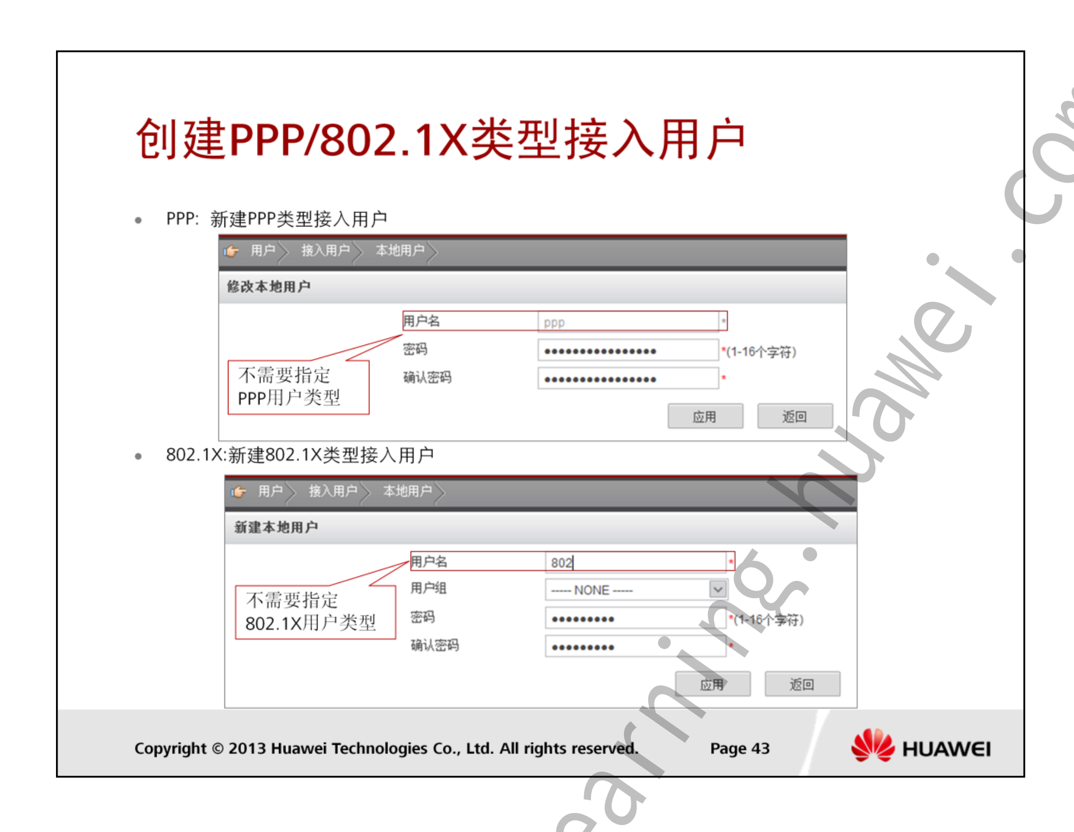
通过在线用户列表，可以查看已经通过设备认证的在线用户。管理员可对在线用户进行相关的管理操作，例如强制注销。

- 查看在线用户
- 只能查看已经通过设备认证的在线用户。
  - 选择“用户 > 上网用户 > 监控”。
  - 在“组织结构”中，使用以下方式的一种来查看指定用户组的在线用户的信息：
- 查看已经通过设备认证的在线用户。
  - 执行命令display user-manage [vpn-instance { public | vpn-instance-name }] online-user [verbose] [group group-name | ip-range start-ip-address end-ip-address | user user-name]，查看在线用户信息。
- 强制注销在线用户
  - 执行命令system-view，进入系统视图。
  - 执行命令user-manage cut online-user [vpn-instance vpn-instance-name] { group group-name | user user-name | ip ip-address }，强制注销在线用户。
- 强制注销全部在线用户
  - 执行命令reset user-manage online-user [vpn-instance { public | vpn-instance-name }]，强制注销全部在线用户



目录





创建PPP/802.1X类型接入用户的命令行参考配置为：

- PPP:

  [USG] aaa

  [USG-aaa] local-user client001 password cipher Admin@123

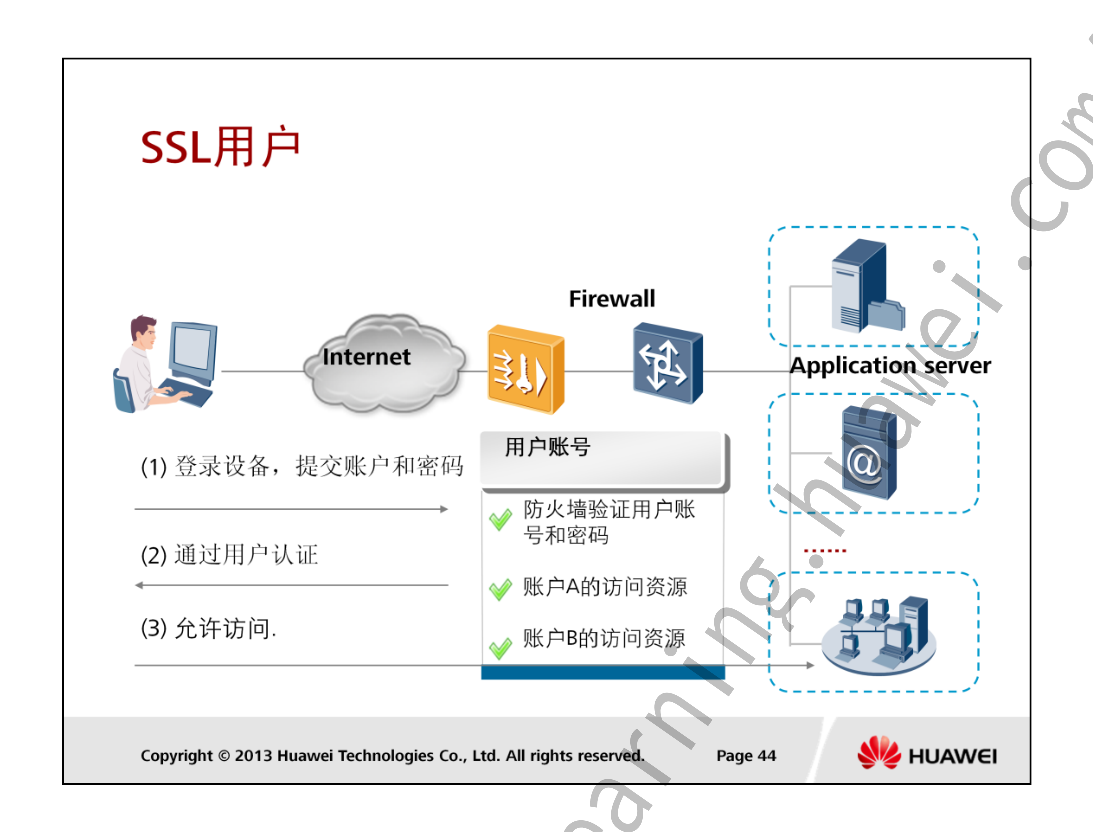
  [USG-aaa] local-user *user-name* service-type ppp

- 802.1X:

  [USG] aaa

  [USG-aaa] local-user client001 password cipher Admin@123

  [USG-aaa] local-user user-name service-type 802.1X



SSL VPN是以HTTPS为基础的VPN技术，工作在传输层和应用层之间，在Internet基础上提供机密性的安全协议。主要提供业务有Web代理、网络扩展、文件共享和端口转发。

- SSL协议通信的握手步骤如下：
  - SSL客户端向SSL服务器发起连接，并要求服务器验证自身的身份。
  - 服务器通过发送自身的数字证书证明身份。
  - 服务器发出一个请求，对客户端的证书进行验证。
  - 验证通过后，协商用于加密的消息加密算法和用于完整性检查的哈希函数。通常由客户端提供它支持的所有算法列表，然后由服务器选择最强大的加密算法。
  - 客户端和服务器通过以下步骤生成会话密钥：
    - 客户端生成一个随机数，并使用服务器的公钥（从服务器证书中获取）对它加密，以送到服务器上。
    - 服务器用随机数据（客户端的密钥可用时则使用客户端密钥，否则以明文方式发送数据）响应。
    - 使用哈希函数从随机数据中生成密钥。



- 认证方式
  - VPNDB本地认证
    - VPNDB用于本地VPN数据库认证。
    - 本地认证的优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
  - 远端认证
    - 支持通过RADIUS协议进行远端认证。
    - 支持通过LDAP协议进行远端认证。
  - 证书认证
    - 支持对证书进行有效性认证。
- 授权方式
  - VPNDB本地授权
    - VPNDB用于本地VPN数据库授权，管理员通过管理用户和组来维护VPNDB。当用户接入时，根据本地配置的用户信息（包括用户名、密码及其他属性）进行授权。
  - 远端授权
    - 支持通过RADIUS和LDAP进行远端授权。



总结

- 用户认证简介
- AAA技术原理
- 用户认证管理及应用



思考题

- 什么是AAA认证，有哪些典型的AAA认证方式?
- 用户管理有哪些分类?
- 单点登录认证流程是什么?



Thank you

www.huawei.com

HC110310007

HCNA-Security-CBSN 第七章 防火墙网络互联技术


第七章
防火墙网络互联技术
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目标

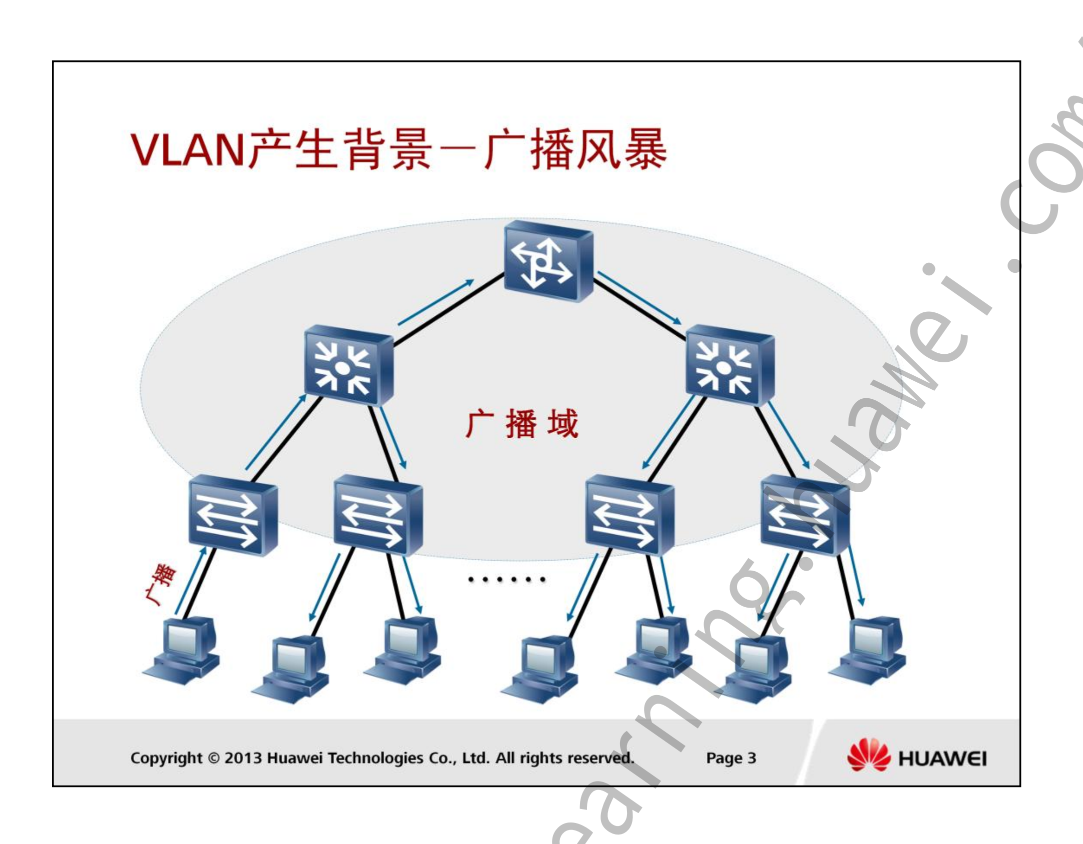
- 学完本课程后，您将能够:
  - 掌握VLAN的基本技术
  - 掌握SA与E1广域接口技术
  - 掌握ADSL的基本技术
  - 掌握WLAN与3G无线技术





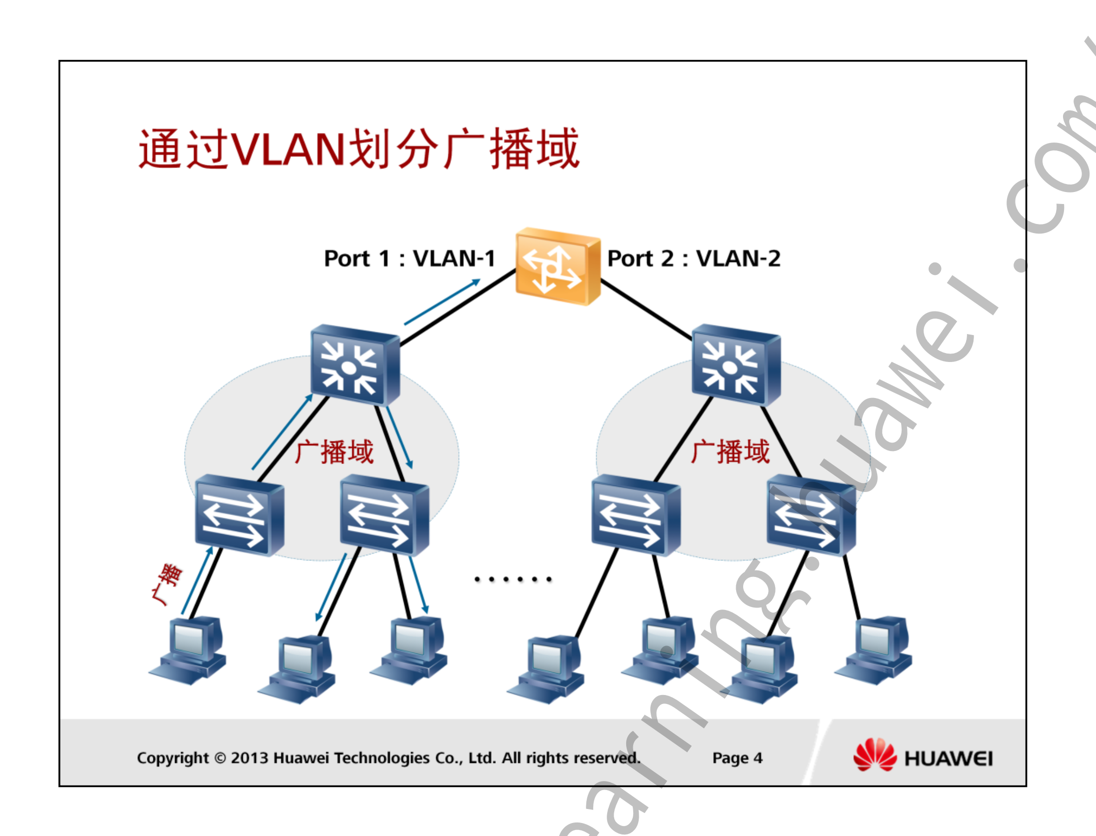
目录





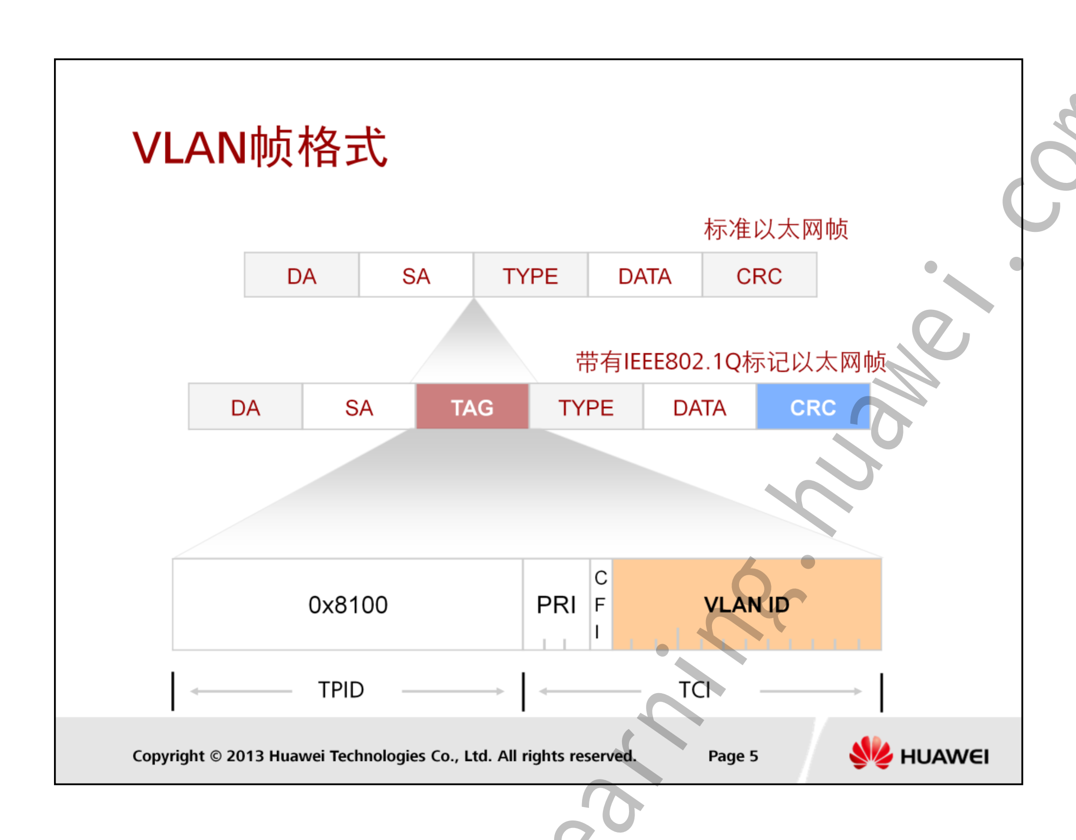
传统的局域网使用的是HUB，HUB只有一根总线，一根总线就是一个冲突域。所以传统的局域网是一个扁平的网络，一个局域网属于同一个冲突域。任何一台主机发出的报文都会被同一冲突域中的所有其它机器接收到。后来，组网时使用网桥（二层交换机）代替集线器（HUB），每个端口可以看成是一根单独的总线，冲突域缩小到每个端口，使得网络发送单播报文的效率大大提高，极大地提高了二层网络的性能。假如一台主机发出广播报文，设备仍然可以接收到该广播信息，我们通常把广播报文所能传输的范围称之为广播域，网桥在传递广播报文的时候依然要将广播报文复制多份，发送到网络的各个角落。随着网络规模的扩大，网络中的广播报文越来越多，广播报文占用的网络资源越来越多，严重影响网络性能，这就是所谓的广播风暴的问题。

由于网桥二层网络工作原理的限制，网桥对广播风暴的问题无能为力。为了提高网络的效率，一般需要将网络进行分段：把一个大的广播域划分成几个小的广播域。



虚拟局域网（VLAN——Virtual Local Area Network）逻辑上把网络资源和网络用户按照一定的原则进行划分，把一个物理上实际的网络划分成多个小的逻辑的网络。这些小的逻辑的网络形成各自的广播域，也就是虚拟局域网VLAN。图中都使用一个中心交换机，但是左右各属于不同的VLAN，形成各自的广播域，广播报文不能跨越这些广播域传送。

虚拟局域网将一组位于不同物理网段上的用户在逻辑上划分成一个局域网内，在功能和操作上与传统LAN基本相同，可以提供一定范围内终端系统的互联。



VLAN实际上是在源和目的MAC与TYPE之间增加了802.1Q TAG标记，包括两个部分TPID和TCI。

- TPID（Tag Protocol Identifier，标签协议标识）VLAN Tag中的一个字段，IEEE802.1Q协议规定该字段的取值为0x8100。
- TCI包含帧的控制信息：
  - priority:指明优先级。一共有0-7的8种优先级；
  - canonical format indicator(CFI):CFI值为0说明是规范格式，值为1是非规范格式。它被用在令牌环/源路由FDDI介质访问方法中来指示封装帧中所带地址的比特次序信息。
  - vlan identified(VLAN ID):这是一个12位的域，指明VLAN的ID，一共4096个，每个支持802.1Q协议的交换机发送出来的数据包都会包含这个域，以指明自己属于哪一个VLAN。

以太网交换机端口分类

- Access端口
- Trunk端口
- Hybrid端口

缺省ID（PVID)作用是什么?

 Page 6 

- Access端口

一般用于接用户计算机的端口，access端口只能属于1个VLAN。

- Trunk端口

一般用于交换机之间连接的端口，trunk端口可以属于多个VLAN，可以接收和发送多个VLAN的报文。

- Hybrid端口

可以用于交换机之间连接，也可以用于接用户的计算机，hybrid端口可以属于多个VLAN，可以接收和发送多个VLAN的报文。

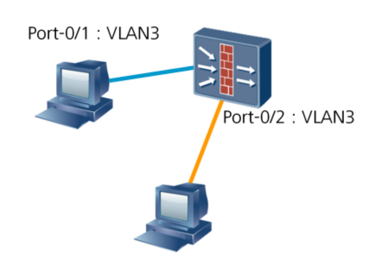
Hybrid端口与Trunk端口的不同之处在于hybrid端口可以允许多个VLAN的报文不打标签，而trunk端口只允许缺省VLAN的报文不打标签。在同一个交换机上hybrid端口和trunk端口不能并存。

端口的缺省ID（PVID）：PVID，全称叫Port VLAN ID，表示端口所属的VLAN。

- Access端口只属于一个VLAN，所以它的缺省ID就是它所在的VLAN，不用设置。
- Hybrid端口和Trunk端口属于多个VLAN， 所以需要设置缺省VLAN ID，缺省情况下为VLAN 1。

Access-Link配置

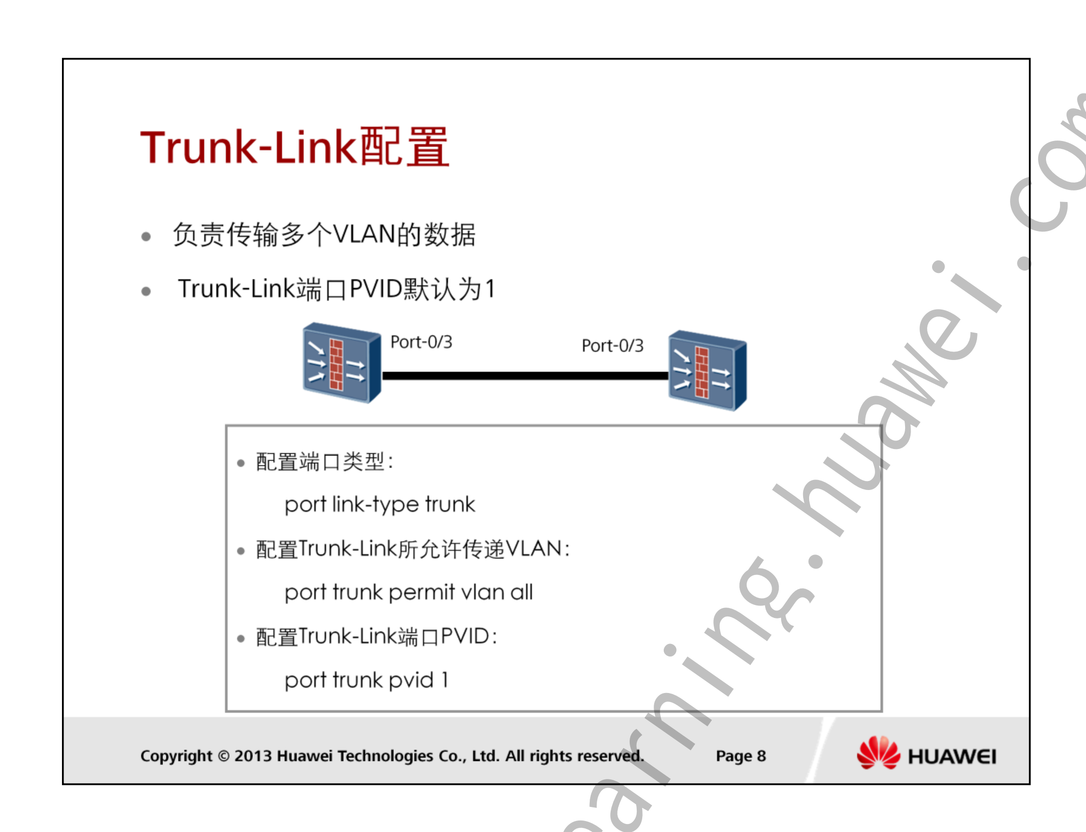
- 默认情况下，交换机所有端口都是Access-Link端口，并属于VLAN-1，即PVID (Port VLAN ID)为1



- 配置端口类型:
  port link-type access
- 创建VLAN:
  vlan 3
- 向VLAN中添加端口:
  port ethernet 0/1
- 或将端口加入VLAN:
  port access vlan 3

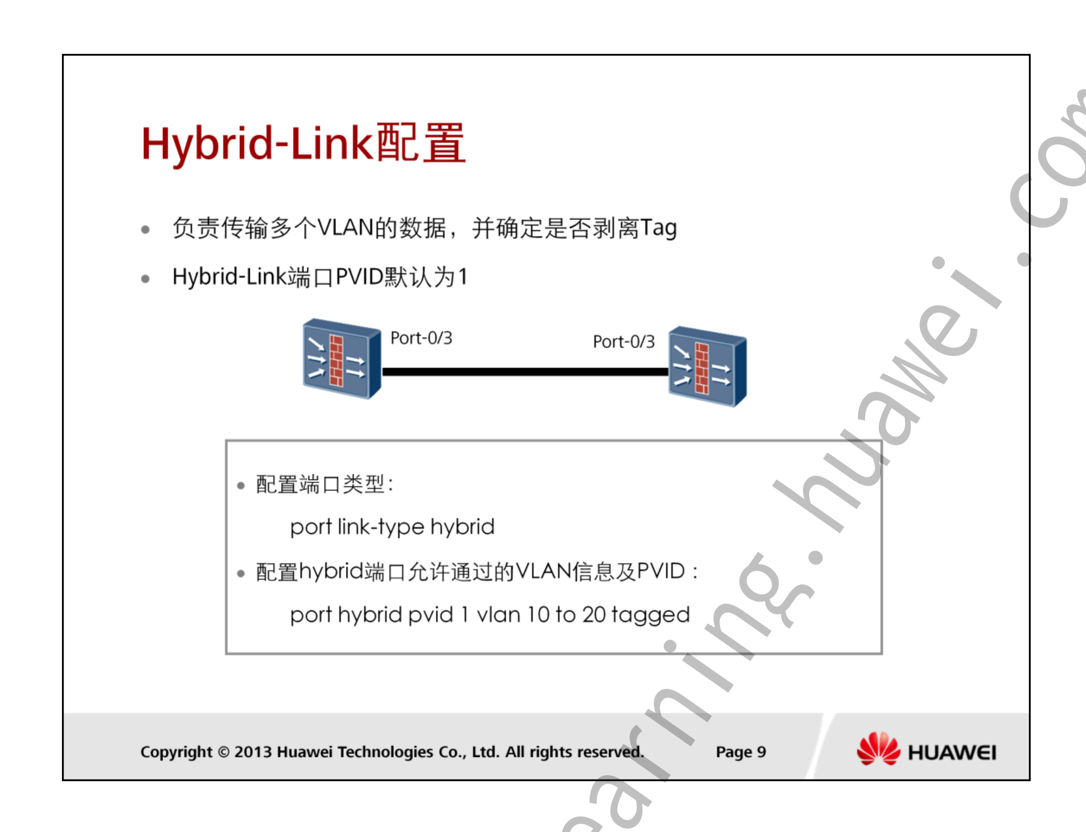


HUAWEI



Trunk端口负责在交换机与交换机之间传递多个VLAN的数据帧，具体允许传递哪些VLAN的数据帧可以通过命令“port trunk permit vlan [VID]”来实现。

这里有条命令“port trunk pvid vlan-id ”具体作用是为改变Trunk端口的PVID值，Trunk端口PVID值的意义与Access端口PVID的意义有点不一样，在Access里表示端口所属的VLAN，但在Trunk里却表示默认VLAN的值。

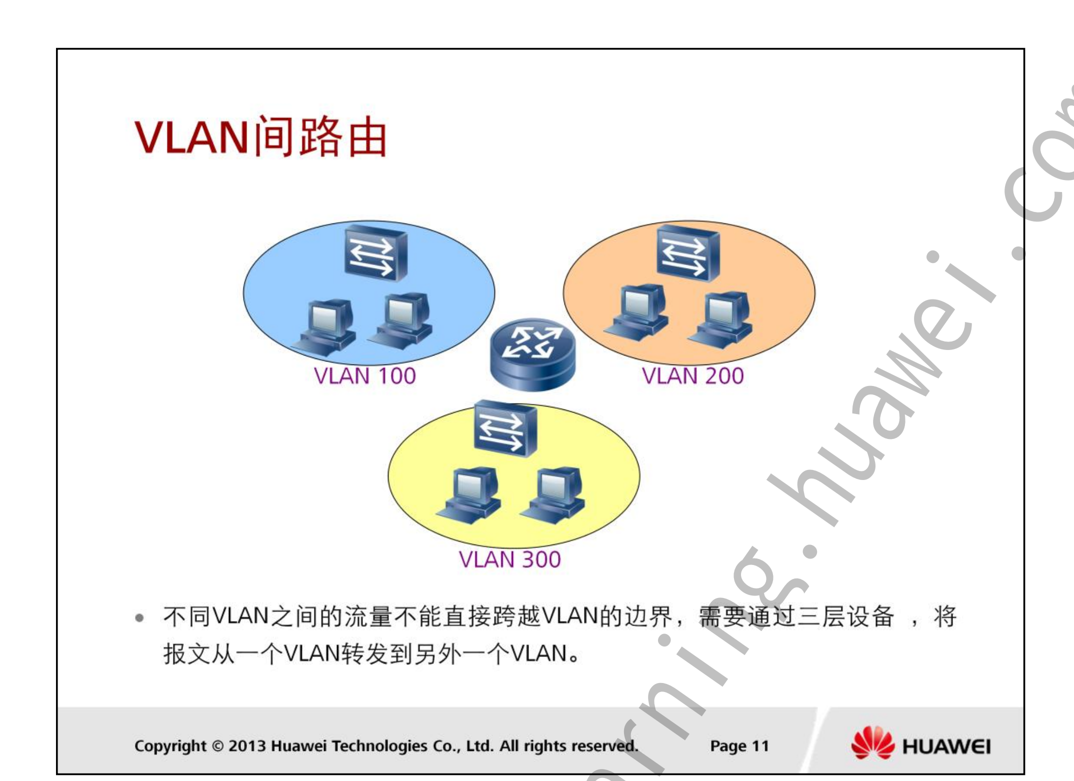


Hybrid端口允许多个VLAN的帧通过，并可以在出端口方向将某些VLAN帧的Tag剥掉。具体允许传递哪些VLAN的数据帧通过且剥离Tag,可以使用下述命令来实现：

port hybrid { pvid vlan-id | vlan { vlan-id1 [to vlan-id2] } & <1–10> { tagged | untagged } }

其中untagged参数代表剥离Tag，而tagged参数代表不剥离Tag。


VLAN接口配置（Web）
选择接口的连接类型
网络 接口 接口
修改Ethernet
接口名称
Ethernet2/0/0
别名
安全区域
trust
模式
路由
交换
连接类型
Access
Trunk
Hybrid
Access VLAN ID
1
<1-4094>
高级
应用
返回
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 10
HUAWEI



不同VLAN间要进行通信，必须通过三层设备如路由器或三层交换机实现。最直接的办法是将不同的VLAN连接到三层设备的不同接口，通过路由实现不同VLAN间的数据通信。但这样会浪费设备上有限的物理接口。为解决这个问题，可以使用子接口。

在一个物理接口上配置多个子接口，这些子接口分别对应不同VLAN，这样只需连接一个物理接口就可实现不同VLAN之间的数据通信。

- 操作步骤

执行命令system-view，进入系统视图。

执行命令interfac interface-type interface-number.subinterface-number，创建子接口并进入子接口视图。

执行命令vlan-type dot1q vlan-id，配置子接口的封装类型及关联的VLAN ID。

执行命令ip address ip-address { mask | mask-length } [sub]，配置子接口的IP地址。子接口的IP地址和主接口的IP地址可以在同一主网段上，但其子网掩码不能相同。



目录



WLAN概述

- WLAN （Wireless Local Area Network，无线局域网)服务内容包括：
  - 应用具有无线局域网功能的设备建立无线网络，带有无线网卡的用户可以连接到无线网络，并能够接入固定网络或因特网。
  - 无线用户可以访问传统802.3局域网。
  - 使用不同认证和加密方式，安全地访问WLAN。
  - 为无线用户提供安全的网络接入和移动区域内的无缝漫游 。



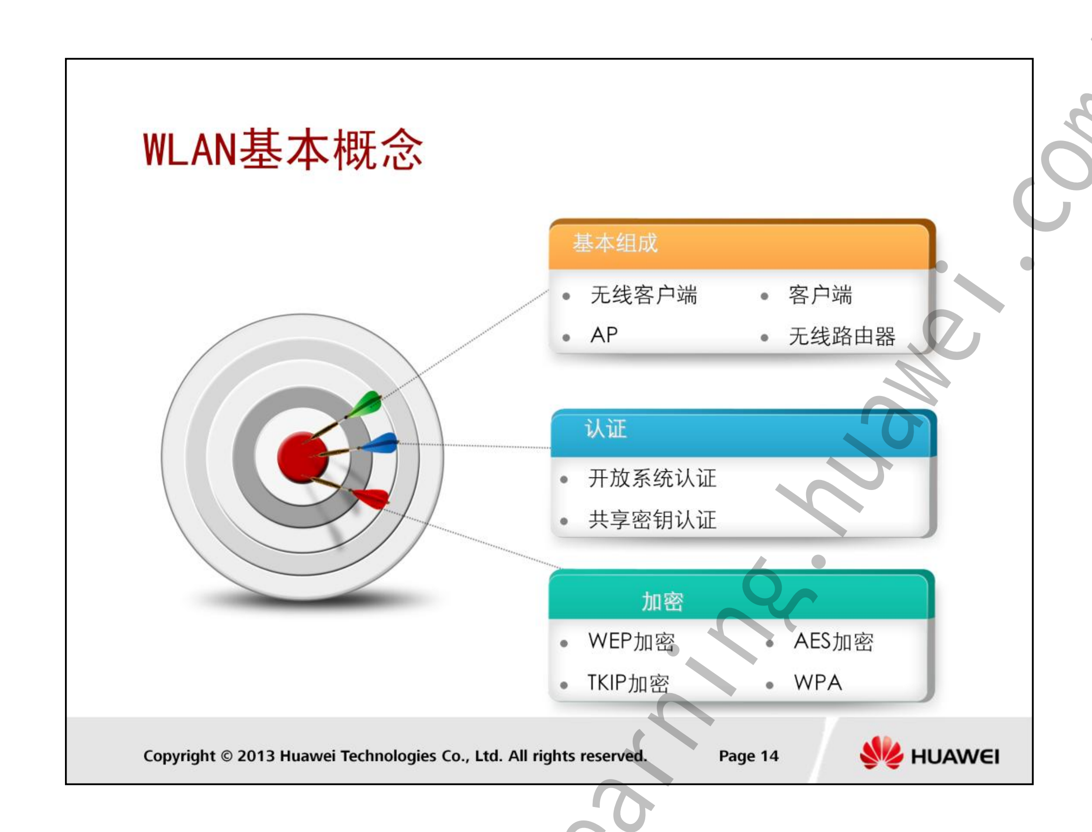
 Page 13



WLAN （Wireless Local Area Network，无线局域网)技术是当今通信领域的热点之一，其主要原因是WLAN系统便于搭建和使用，部署时不需要考虑复杂的布线和变迁。然而，WLAN系统不是完全的无线系统，它的服务器和骨干网仍然安置在固定网络，只是用户可以移动。

802.11协议提供的无线安全性能可以很好地抵御一般性网络攻击，但是仍有少数黑客能够入侵无线网络，从而无法充分保护包含敏感数据的网络。为了更好的防止未授权用户接入网络，需要实施一种性能高于802.11的高级安全机制。

USG2000系统通过合入WLAN安全特性，来增强系统的安全性和健壮性。该特性通过检查WLAN-MAC的方式提供802.11客户端的安全接入 。



- 无线客户端（STA）

  在一个网络中，所有的连接到无线介质的设备都可以称之为无线客户端。每一个无线客户端都装有支持802.11的无线网卡。无线客户端可以分为两大类：AP和客户端。

- AP（Access Point，接入点）

  AP提供无线用户到局域网的桥接功能，在用户同局域网间进行无线到有线和有线到无线的帧转换。 我们的USG2100/2200就是个AP接入点。

- 客户端

  可以是便携式笔记本电脑、个人数字助理、IP电话、台式机或者装有无线网卡的工作站等其他固定设备。

- 无线路由器

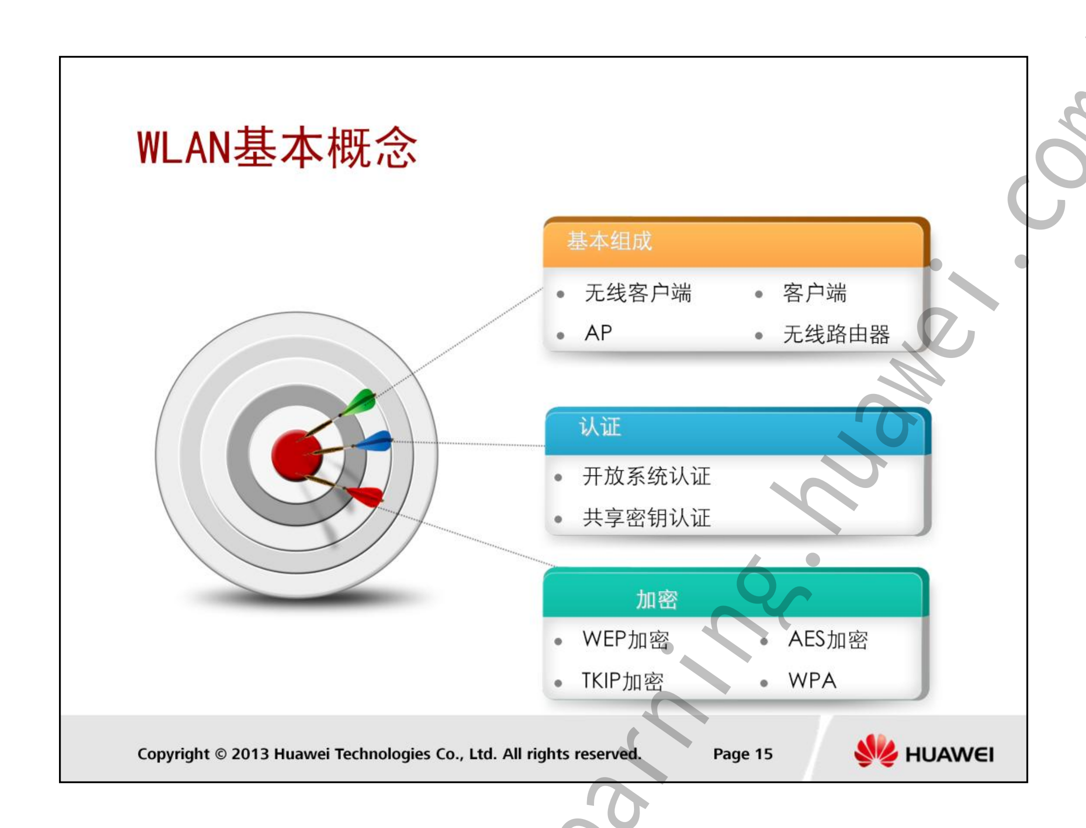
  能提供无线接入功能的路由器，如一台提供三层接口并可作为Fat AP的路由器。所有的无线客户端可以通过无线路由器连接到有线网络、固定网络或者互联网。在本文档中，Fat AP和无线路由器的概念是可以互换的。

- 开放系统认证（Open system authentication）

  开放系统认证是缺省使用的认证机制，也是最简单的认证算法，即不认证。如果认证类型设置为开放系统认证，则所有请求认证的客户端都会通过认证。

- 共享密钥认证（Shared key authentication）

  共享密钥认证是除开放系统认证以外的另外一种认证机制，主要用于pre-RSN设备。这种认证机制只有在使用WEP加密时才可用。用来兼容老的设备。



- WEP加密

  WEP（Wired Equivalent Privacy，有线等效加密）用来保护无线局域网中的授权用户所交换的数据的机密性，防止这些数据被随机窃听。

- TKIP加密

  TKIP是一种加密方法，用于增强pre-RSN硬件上的WEP协议的加密的安全性，其加密的安全性远远高于WEP。

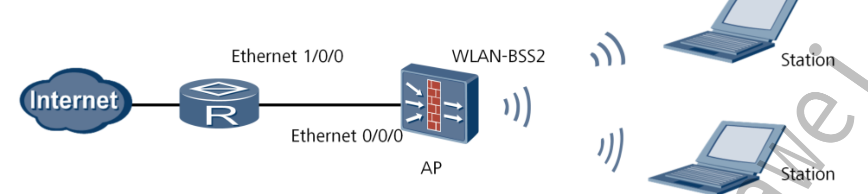
- AES加密

  AES（Advanced Encryption Standard，高级加密标准）加密机制仅用于RSNA客户端。CCM结合CTR（Counter mode，计数器模式）进行机密性校验，级别最高。

- WPA

  Wi-Fi保护访问（Wi-Fi Protected Access，WPA）是一种使无线电脑网络更安全。WPA实现了IEEE 802.11i的主要标准。WPA改进了WEP的认证和加密特性。

WLAN配置举例（命令行）



- 组网需求
  - AP通过Ethernet0/0/0接口（已经加入非信任区域）连接Router。
  - Ethernet0/0/0有固定IP地址：202.169.10.1/24；Router上Ethernet1/0/0的IP地址为202.169.10.2/24。
  - Station的IP地址分别为192.168.1.2/24和192.168.1.3/24。
  - Station使用无线网卡连接到AP（USG），SSID为WLAN100。
  - 使用WPA2-PSK认证模式，CCMP加密套件，预共享（PSK）密钥为abcdefgh
  - 要求通过配置WLAN，实现Station的无线上网

 Page 16



WLAN配置举例（Web）

- 无线服务的安全模式：
  - 不加密
  - WEP
  - WPA、WPA2
  - WPA-PSK、WPA2-PSK
  - WPA-WPA2
  - WPA-WPA2-PSK

采用加密方式的安全模式。

HUAWEI

在Web配置界面中，配置WLAN的操作步骤如下：

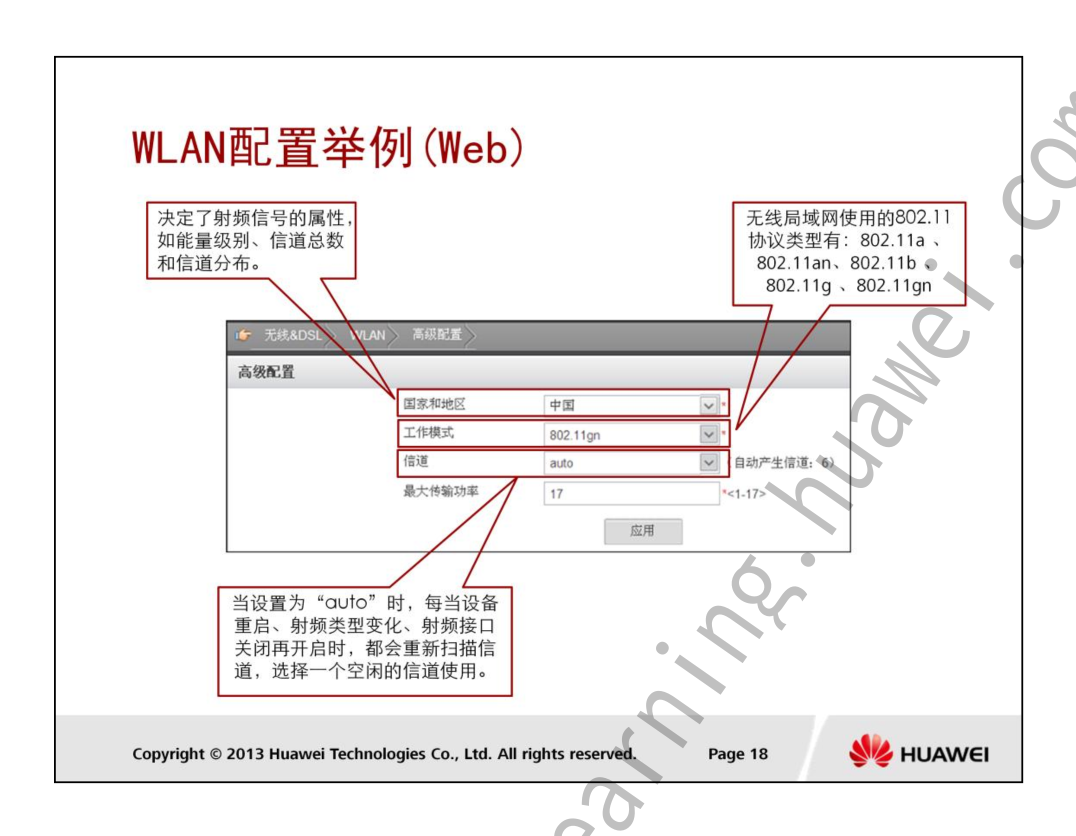
1. 选择“无线&DSL > WLAN > 基本配置”。
2. 选中“无线网络功能”对应的“启用”。如果无线网络功能已经启用，请忽略本步骤
3. 单击“无线服务列表”中的“新建”。
4. 依次输入或选择各项参数。
5. 单击“应用”。

SSID为服务集的名称，无线工作站必须配置与AP相同的SSID才能访问AP。

开启SSID广播后，任何无线用户都可以搜索到该无线网络的存在，容易受到攻击。关闭SSID广播后，这样无线用户就无法搜索到网络名称，从而提高网络的安全。对于专业用户，还是可以通过黑客软件搜索到SSID。如果想最大程度提高网络安全，建议配置高级的安全模式并启用数据加密。建议在配置无线网络的时候，开启SSID广播；配置完成（网络调测通过）后，关闭SSID广播。

WLAN的命令行配置参考如下：

```
[USG] interface Vlanif 2                    //创建Vlanif 2接口。
[USG-Vlanif2] ip address 192.168.1.1 24
[USG] interface wlan-bss 2                  //配置WLAN-BSS接口
[USG-Wlan-Bss2] port access vlan 2
```



在Web配置界面中，配置WLAN的高级选项步骤为：

1. 选择“无线&DSL > WLAN > 高级配置”。
2. 依次输入或选择各项参数。
3. 单击“应用”。

信道号取值范围会随国家和地区代码、射频类型的不同而不同。当设置为“auto”时，每当设备重启、射频类型变化、射频接口关闭再开启时，都会重新扫描信道，选择一个空闲的信道使用。

在设置射频接口的最大传输速率时，较大的传输功率，可以将无线信号覆盖的范围更大，方便远端的无线客户端接入。不要将射频接口的传输功率设置过大，这样可以避免本AP与其他AP间发送冲突和干扰，并且由于传输功率的减弱，可以将无线信号的传输范围控制在本地区域，在一定程度上可以提高无线网络安全性。

```
[USG] wlan service-class 2 crypto              //配置服务类
[USG-wlan-sc-2] ssid WLAN100
[USG-wlan-sc-2] authentication-method wpa2-psk
[USG-wlan-sc-2] encryption-suite ccmp
[USG-wlan-sc-2] pre-shared-key pass-phrase abcdefgh
```

```
[USG-wlan-sc-2] service-class enable

[USG] interface wlan-rf 4/0/0                    //配置射频接口

[USG-Wlan-rf4/0/0] radio-type dot11gn

[USG-Wlan-rf4/0/0] bind service-class 2 interface wlan-bss 2
```

最后，配置无线接收客户端，无线网卡上的SSID、加密方式、预共享（PSK）密钥应与USG设备上保持一致。

WLAN的命令行配置参考如下：

```
[USG] interface Vlanif 2                         //创建Vlanif 2接口。

[USG-Vlanif2] ip address 192.168.1.1 24

[USG] interface wlan-bss 2                       //配置WLAN-BSS接口

[USG-Wlan-Bss2] port access vlan 2

[USG] wlan service-class 2 crypto                //配置服务类

[USG-wlan-sc-2] ssid WLAN100

[USG-wlan-sc-2] authentication-method wpa2-psk

[USG-wlan-sc-2] encryption-suite ccmp

[USG-wlan-sc-2] pre-shared-key pass-phrase abcdefgh
[USG-wlan-sc-2] service-class enable

[USG] interface wlan-rf 4/0/0                    //配置射频接口

[USG-Wlan-rf4/0/0] radio-type dot11gn

[USG-Wlan-rf4/0/0] bind service-class 2 interface wlan-bss 2
```

最后，配置无线接收客户端，无线网卡上的SSID、加密方式、预共享（PSK）密钥应与USG设备上保持一致。

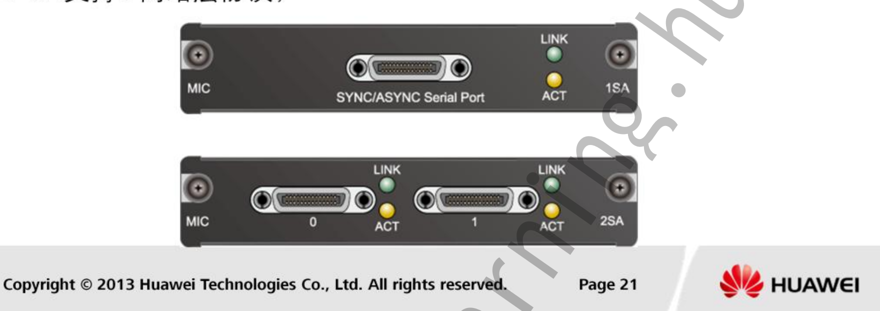


目录



什么是SA串口

- 串口是最常用的广域网接口之一，分为同步串口和异步串口；
- SA可以工作在DTE和DCE两种方式；
- SA作为上行接口，链路上可以承载多种类型的业务，如HTTP、FTP等；
- SA支持的链路层协议类型包括PPP、HDLC；
- SA支持IP网络层协议；



串口是最常用的广域网接口之一，分为同步串口和异步串口。现在应用广泛的是同步串口。

SA接口为同步串口，支持V2.4、V3.5、X.21、RS449、RS530式线缆，其波特率有多种选择，以适应不同的对端设备，最大带宽为2.048Mb/s，适合运营商和一般企业客户的业务数据传输需求。其典型组网为SA接口作为上行口承载业务，企业通过向运营商租用一条SA的专线来连接广域网或行业网。

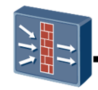
SA 可以工作在DTE（Data Terminal Equipment）和DCE（Data Circuit-terminal Equipment）两种方式。一般情况下，SA作为DTE 设备，接受DCE 设备提供的时钟。

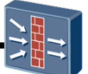
SA作为上行接口，链路上可以承载多种类型的业务，如HTTP、FTP等。为了有效利用上行带宽，需要与QoS一起使用。同时，USG2200支持L2TP和IPSec VPN特性，SA口可以作为VPN隧道的一端，承载L2TP和IPSec隧道。

SA串口-配置举例-命令行方式

USG2200 B

USG2200 A





- 配置USG 2200A

#配置serial1/0/0接口，封装协议采用PPP，其他采用默认值

```
<USG2200A>system-view
[USG2200A]interface serial 1/0/0
[USG2200A-serial1/0/0]ip address 10.110.1.11 255.255.255.0
[USG2200A-serial1/0/0]link-protocol ppp
[USG2200A-serial1/0/0]shutdown
[USG2200A-serial1/0/0]undo shutdown
```

注意：配置完毕后，要将serial1/0/0接口加入安全域中，并打开域间默认包过滤规则。

 Page 22



USG2200 B配置：

#配置Serial1/0/0端口，封装协议采用PPP，其他采用默认值

```
<USG2200 B>system-view
[USG2200 B]interface serial 1/0/0
[USG2200 B-serial1/0/0]ip address 10.110.1.10 255.255.255.0
[USG2200 B-serial1/0/0]link-protocol PPP
[USG2200 B-serial1/0/0]shutdown
[USG2200 B-serial1/0/0]undo shutdown
```

SA串口-配置举例(Web)

网络 > 接口 > 接口

修改Serial

接口名称	Serial4/0/0 *
别名	
VPN实例	public *
安全区域	-NONE-
链路层协议	◉ PPP ○ HDLC
类型	◉ 无 ○ 客户端 ○ 服务器
IP地址	
子网掩码	
NAT功能	☐ 启用
☐ 启用访问管理	☐ HTTP ☐ HTTPS ☐ Ping ☐ SSH ☐ SNMP ☐ Telnet

高级

接口封装的链路层协议为“PPP”或者“HDLC”。

选中“启用访问管理”，表示启用接口访问控制管理。

 Page 23 HUAWEI

在Web配置界面中，配置SA串口的步骤为：

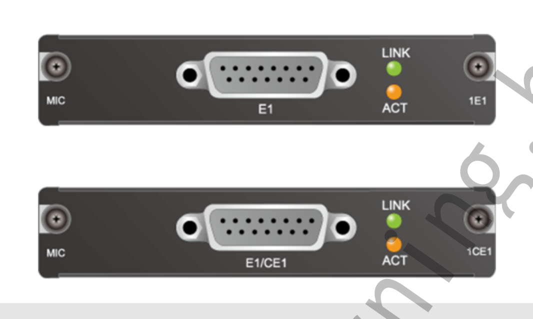
1. 选择“网络 > 接口 > 接口”。
2. 点击Serial接口后方的编辑框，进入串口编辑视图。
3. 依次输入各项参数。

选中“启用访问管理”，表示启用接口访问控制管理，允许用户通过HTTP、HTTPS、Ping、SSH、SNMP以及Telnet访问接口，对设备实施管理。

通过启用访问管理配置的访问控制，其优先级高于其他方式包过滤。在不选中“启用访问管理”的情况下，设备会根据本地策略来判断报文是否允许通过。

什么是E1/cE1

- E1接口是广泛应用的低速WAN物理接口，处于PDH速率体系的底层，通过不同的应用模式为用户提供灵活的低速接入方式。
- USG支持的E1有两种模式：E1模式和CE1模式，在E1模式下所有时隙都被用于传输数据；在CE1模式下，为31路PCM，其中16号时隙也被用于传输数据。



Page 24



现在的数字传输系统都采用脉码调制PCM（Pulse Code Modulation）体制。PCM最初是为了使电话局之间一条中继线不只传送一路而是可以传送多路电话而设计的。欧洲的30路PCM，简称为E1。E1有32个时隙TS（Time Slot），其中有30路时隙用来传输数据，0号时隙传输帧同步和告警信令，16号时隙传输控制信令。E1的最大速率是2.048Mbit/s。

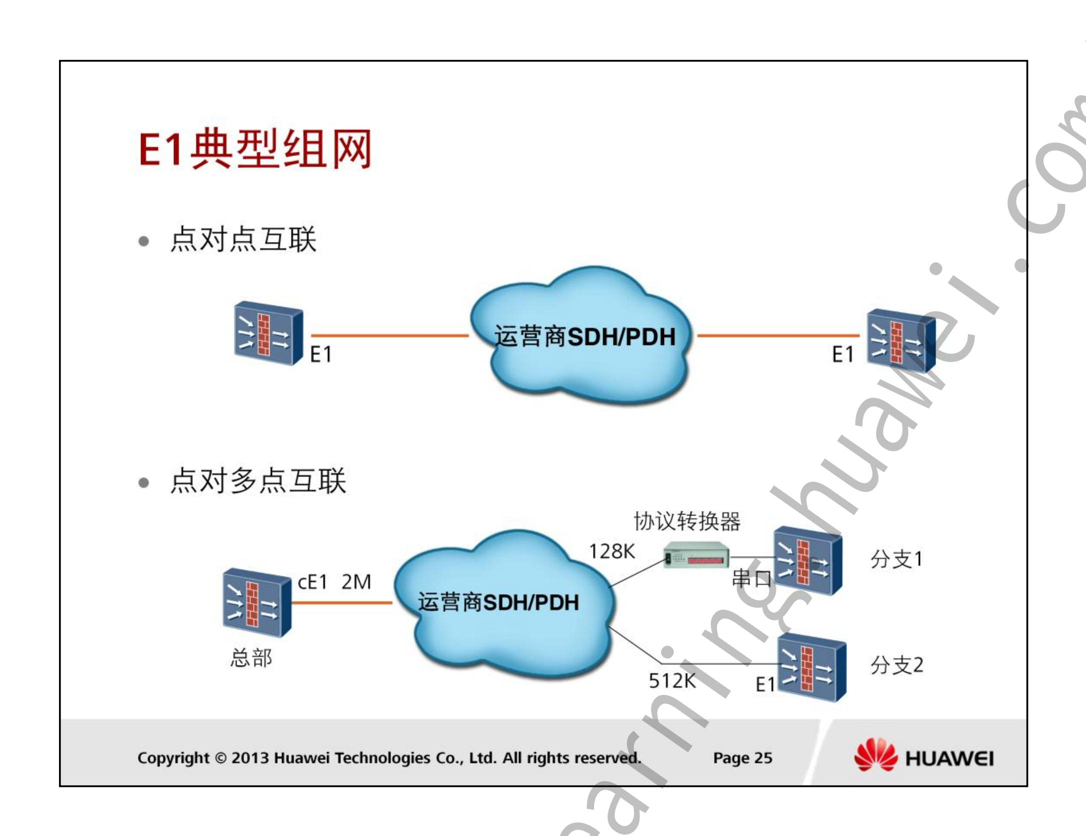
E1接口的本质是时分复用（TDM）。E1接口具有多种应用模式：非通道化（仅E1支持）/通道化/部分通道化/PRI。E1接口的物理特性包括：时钟、编码、帧格式、帧同步、空闲码、帧间填充、环回。

E1接口可以将所有时隙或除帧头以外的所有时隙捆绑为一个逻辑接口，该逻辑接口与同步串口具有相同的逻辑特性。

CE1接口可以将所有时隙捆绑为一个逻辑接口，或将除帧头以外的所有时隙捆绑为多个逻辑接口，每个逻辑接口与同步串口都具有相同的逻辑特性。

E1接口只能工作在净通道模式或非通道化模式，CE1接口只能工作在净通道模式或通道化模式。通道化、非通道化、净通道概念如下：

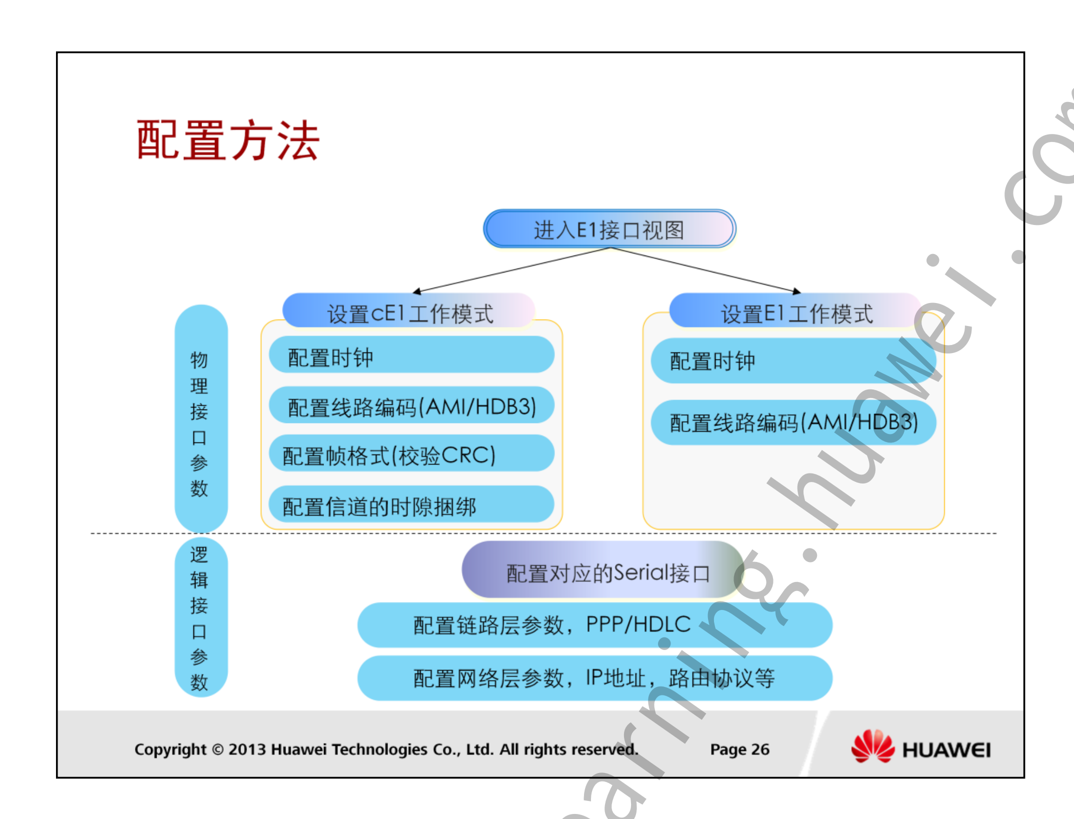
- 通道化（Channelized）：指在成帧模式（Framed）下，数据码流（E1、T1、E3、DS3等）除帧头以外的时隙可以分配到多个通道内。
- 非通道化（Unchannelized）：指在成帧模式（Framed）下，数据码流除帧头以外的所有时隙只能被绑定一次，分配到一个通道内。
- 净通道（Clear Channel）：也称为非成帧模式（Unframed），即数据码流没有定帧信号，码流里的任意比特都是数据。当然，码流里的数据也只能属于一个通道。



在E1点对点互联型组网中，可以有三种对接方式：

- E1接口互联
- E1接口通过协议转换器与对端设备串口相连
- 两端设备的串口通过协议转换器与对端相连

在点对多点互联型组网中，总部设备出接口可以为2M E1接口或者155M的cPOS接口，根据总部接口的不同，对端设备的接口速率也会有所差异。



- 物理接口配置

```
controller e 9/0/0
clock master
code hdb3
frame-format  no-crc4
using ce1
channel-set 0 timeslot-list 1-4
channel-set 1 timeslot-list 5-8
```

- 逻辑接口配置

```
interface Serial9/0/0:0
link-protocol ppp
ip address 100.1.1.1 255.255.255.252
#
interface Serial9/0/0:1
link-protocol ppp
ip address 110.1.1.1 255.255.255.252
#
```

E1/cE1配置举例(Web)

新建 删除 刷新 请选择查询类别 查询

接口名称	安全区域	IP地址	VLAN Tag	模式	连接类型	状态(物理/协...	启用	配置
E1 1/0/0								

网络 > 接口 > 接口

修改E1

接口名称 E1 1/0/0 *

别名

当前E1模式 非成帧 成帧

线路编解码格式 AMI HDB3

帧格式 CRC4 NO-CRC4

时钟模式 主时钟 从时钟

时隙捆绑 时隙捆绑配置

时隙捆绑结果

应用 返回

点击该图标进入E1接口修改界面，但接口名称不能修改。

该参数只在“当前E1模式”为“成帧模式”时需要配置。

 Page 27 HUAWEI

在Web配置界面下，E1/cE1的配置步骤为：

1. 选择“网络 > 接口 > 接口”。
2. 单击E1接口所在行的配置项。
3. 重新输入或选择各项参数。其中，“接口名称”不可修改。
4. 单击“应用”。

为E1/CE1接口配置时隙捆绑时。该参数只在“当前E1模式”为“成帧模式”时需要配置。配置方法如下：

1. 单击“时隙捆绑配置”，选择或输入各项参数，
2. 捆绑模式：配置E1/CE1接口的时隙捆绑模式。
3. 单击“添加”。如果操作成功，“时隙捆绑结果”中将添加新配置项。
4. 单击“确定”。

什么是ADSL？

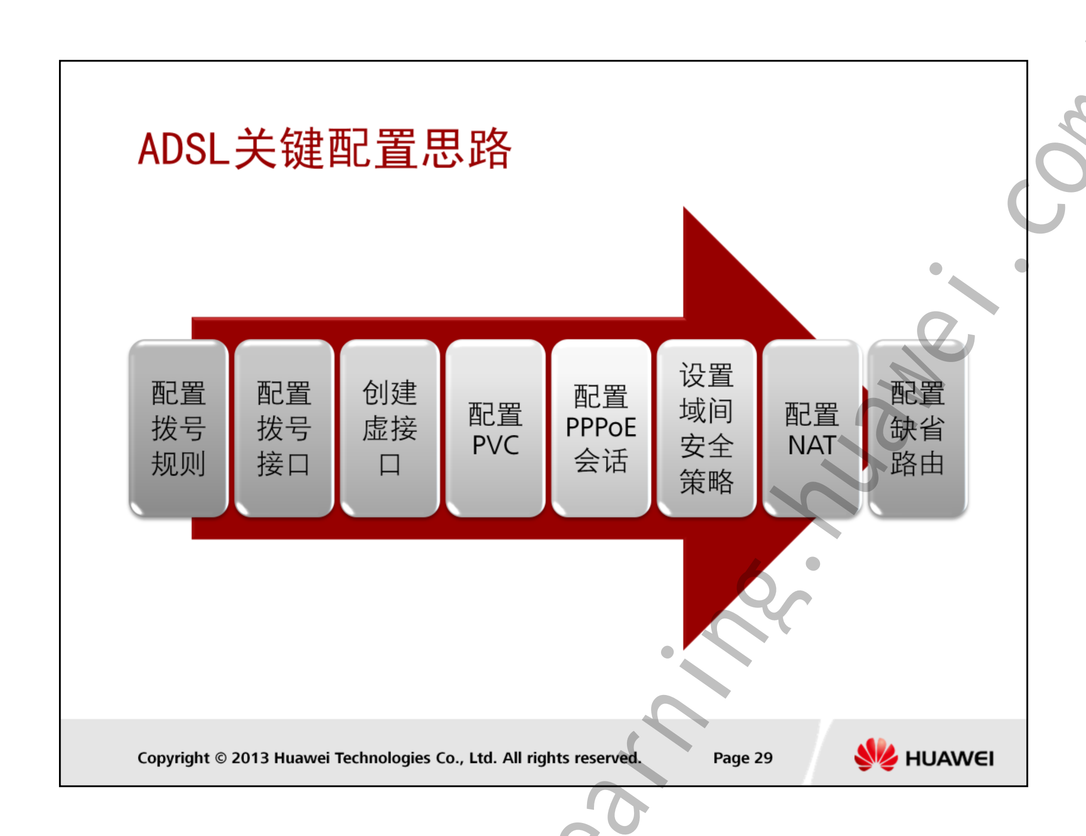
- ADSL（Asymmetric Digital Subscriber’s Line）：
  - 非对称数字用户线路,其特点是从服务提供商到用户端（下行）与从用户端到服务提供商（上行）具有不同的数据速率。
- ADSL下行传输速率最大可以达到8Mbps，上行传输速率最大可以达到896kbps，由于ADSL的下行速率不等于且远远大于上行速率，所以被称作非对称DSL技术。



Page 28



ADSL在一对电话线上同时承载语音业务和数据业务，利用现有的PSTN网络设施，采用特殊的调制技术，在保证不影响正常电话使用的前提下，利用原有的电话双绞线进行高速数据传输。实现用户接入网络运行数据业务的需求。



ADSL配置参考命令如下:

[USG] dialer-rule 1 ip permit //**配置拨号规则**

[USG] interface Dialer 1 //创建Dialer接口，并进入Dialer视图。

[USG-Dialer1] dialer user USG //指定要拨号的远端用户名。

[USG-Dialer1] dialer bundle 1 //指定拨号口使用的dialer bundle。

[USG-Dialer1] dialer-group 1 //配置Dialer 1接口所属的拨号访问组。

[USG-Dialer1] link-protocol ppp // 配置链路层协议为PPP。

[USG-Dialer1] ip address ppp-negotiate // 使用协商方式获取IP地址

[USG-Dialer1] ppp ipcp dns admit-any // 使用协商方式获取DNS地址

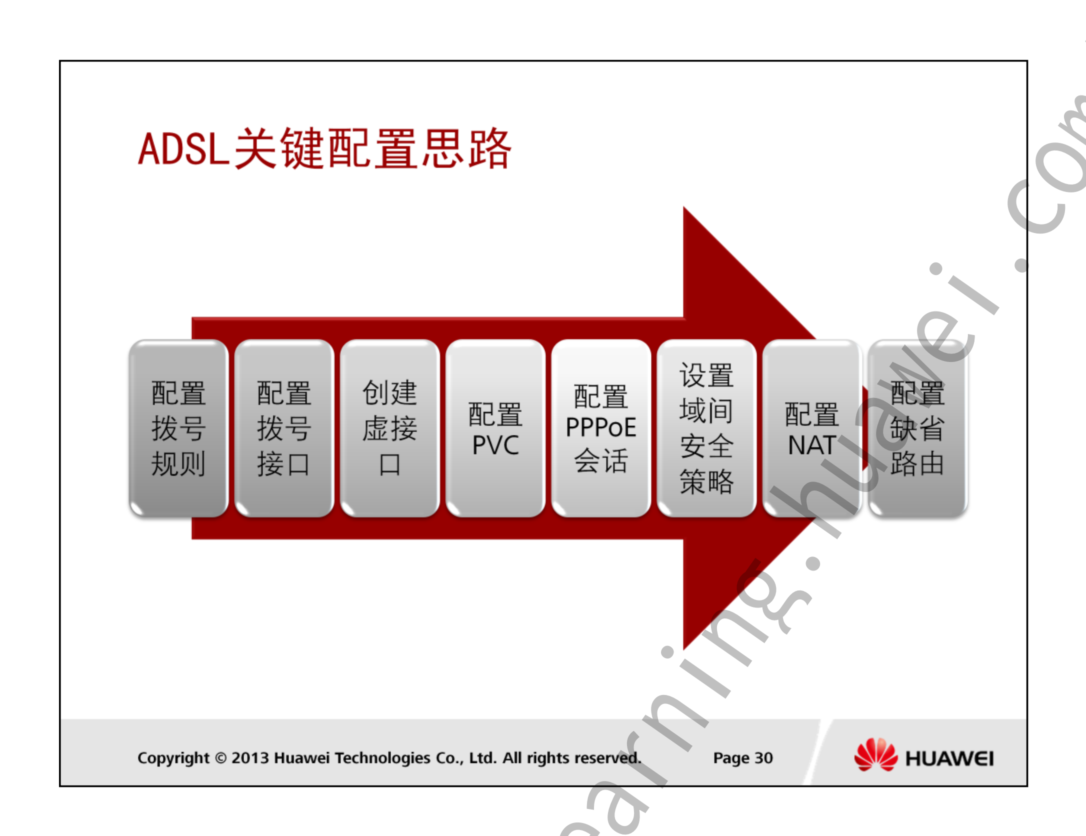
[USG-Dialer1] ppp pap local-user Abcdefgh~ password simple Abcdefgh~

//使用PAP认证方式，用户名和密码均Abcdefgh~

[USG-Dialer1] quit //退回系统视图。

[USG] interface Virtual-Ethernet 1 //创建接口Virtual-Ethernet 1。

[USG-Virtual-Ethernet1] quit



[USG] interface Atm2/0/0 //配置接口Atm 2/0/0

[USG-Atm2/0/0] PVC 8/35 //配置接口Atm 2/0/0的PVC值

[USG-Atm2/0/0-8/35] map bridge virtual-ethernet 1 //配置与虚接口映射

[USG-Atm2/0/0-8/35] encapsulation llc //配置PVC的封装类型为LLC

[USG] interface Virtual-Ethernet 1 //配置PPPoE会话。

[USG-Virtual-Ethernet1] pppoe-client dial-bundle-number 1

[USG] interface Vlanif 1 //将Vlanif接口和Dialer接口分别加入安全区域。

[USG-Vlanif1] ip address 192.168.0.1 24

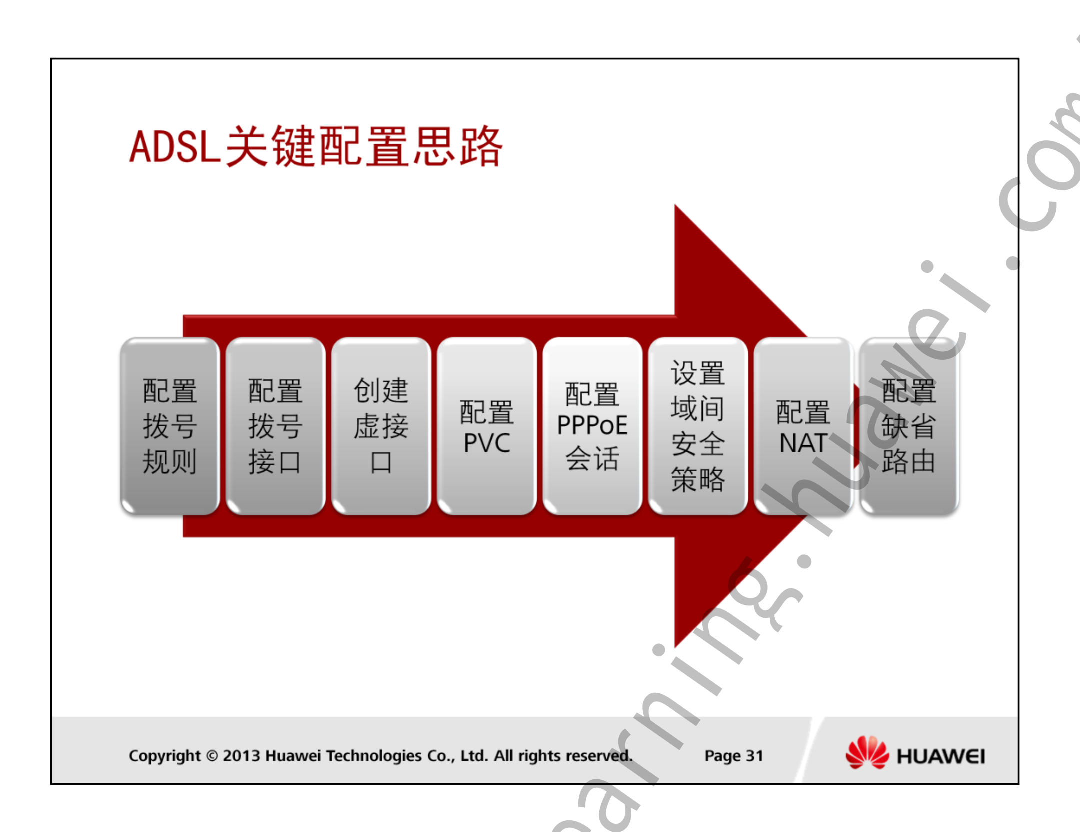
[USG-Vlanif1] quit

[USG] firewall zone trust

[USG-zone-trust] add interface Vlanif 1

[USG] firewall zone untrust //将Dialer 1接口加入Untrust域。

[USG-zone-untrust] add interface Dialer



- 对于USG系列，配置域间包过滤，以保证网络基本通信正常。对于USG BSR/HSR系列，不需要执行此步骤。

  [USG] policy interzone trust untrust inbound

  [USG-policy-interzone-trust-untrust-inbound] policy 0

  [USG-policy-interzone-trust-untrust-inbound-0] action permit

- 配置NAT和缺省路由。

  [USG] nat-policy interzone trust untrust outbound

  [USG-nat-policy-interzone-trust-untrust-outbound] policy 1

  [USG-nat-policy-interzone-trust-untrust-outbound-1] action source-nat

  [USG-nat-policy-interzone-trust-untrust-outbound-1] policy source 192.168.0.0 0.0.0.255

  [USG-nat-policy-interzone-trust-untrust-outbound-1] easy-ip Dialer 1

- 配置缺省路由。

  [USG] ip route-static 0.0.0.0 0.0.0.0 Dialer 1

ADSL关键配置举例(Web)

无线&DSL > XDSL > XDSL2/0/0

配置 XDSL2/0/0

接口名称 XDSL2/0/0

XDSL功能 启用

应用

新建PVC配置

当前状态：未连接

基本配置

接口名称 XDSL2/0/0

XDSL功能 启用

用户名

密码

PVC(VPI/VCI) *<0-255> / *<32-65535>

封装类型 LLC

在线方式 一直在线 / 空闲自动断线（秒） *<1-65535>

安全区域 untrust

NAT功能 启用

高级

应用 返回

这部分参数需要根据运营商相应的参数进行配置。

一直在线：适用于不计流量、不计时间的场合；空闲自动断线（秒）：适用于对流量和链路使用时间敏感的场合。

 Page 32 HUAWEI

在Web配置界面中，ADSL的配置步骤如下：

1. 选择进入“无线&DSL > XDSL > XDSL接口编号”视图界面。
2. 选中“XDSL功能”对应的“启用”。
3. 单击“应用”。
4. 单击“PVC配置列表”中的“新建”。
5. 依次输入或选择各项参数。
6. 单击“应用”。

选择在线方式，既选择拨号方式，USG防火墙提供两种拨号方式：

- “一直在线”

链路建立后，当链路没有业务流量时，设备会发送保活报文来维持链路Up。

- “空闲自动断线（秒）”

只有存在数据需要传送时，设备才会触发建立链路。当链路没有流量的时间到达超时时间后，设备会拆除链路，以节约流量。

什么是3G

- 3G是Third Generation的缩写，全称第三代移动通信系统。
- 3G的标准
  - WCDMA
  - TD-SCDMA
  - CDMA2000



 Page 33 

3G是Third Generation的缩写，全称第三代移动通信系统，最早由国际电信联盟ITU于1985年提出，该系统工作在2000MHz频段，最高业务速率可达2000kbit/s。

3G标准有WCDMA（欧洲版）、CDMA2000（美国版）和TD-SCDMA（中国版）。CDMA是Code Division Multiple Access (码分多址)的缩写，是第三代移动通信系统的技术基础。

WCDMA，全称为Wideband CDMA，也称为CDMA Direct Spread，意为宽频分码多重存取，这是基于GSM网发展出来的3G技术规范。

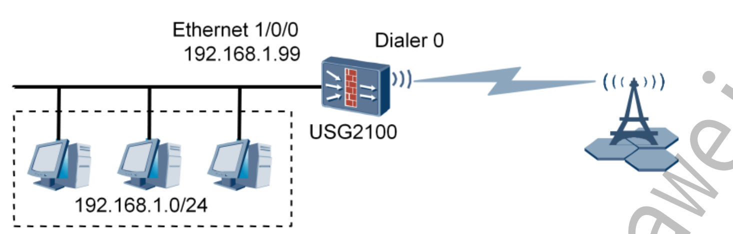
CDMA2000是由窄带CDMA(CDMA IS95)技术发展而来的宽带CDMA技术，也称为CDMA Multi-Carrier。目前中国电信正在采用这一方案向3G过渡，并已建成了CDMA IS95网络。

TD-SCDMA全称为Time Division - Synchronous CDMA(时分同步CDMA)，该标准是由中国大陆独自制定的3G标准。

3G能实现很多移动业务:

- 宽带上网
- 视频通话
- 手机电视
- ……

3G应用配置举例－命令行方式



- 场景描述
  - USG2200使用Ethernet 1/0/0接口连接企业内部网络，使用USB 3G 5/0/0接口接入Internet。
- 组网要求：
  - 企业内网所在网段为192.168.1.0/24。
  - 使用Dialer 0接口进行按需拨号。
  - Express-3G接口的IP地址由无线网络协商分配。





3G应用配置举例，（命令行配置，以联通为例）：

```
firewall packet-filter default permit  all
 dialer-rule 1 ip permit
interface Dialer0
 link-protocol ppp   //TD-SCDMA、WCDMA无需配置PPP认证；
ppp ipcp dns admit-any
 ip address ppp-negotiate
 dialer enable-circular
 dialer-group 1   //此序号应与相应dialer-rule 的序号一致
dialer timer idle 60
 dialer timer autodial 10
 dialer number *99# autodial   //WCDMA的拨号串是*99#
interface Cellular5/0/0
 apn UNINET   //WCDMA制式配置为UNINET；TD-SCDMA制式需配置为 CMNET；
link-protocol ppp
 dialer circular-group 0   //此序号应与相应dialer接口的序号一致
ip route-static 0.0.0.0 0.0.0.0 Dialer0
```

3G应用配置举例(Web)

 Page 36 HUAWEI

在Web配置界面中，3G应用的配置步骤如下：

1. 选择进入“无线&DSL > 3G > 3G配置”视图。
2. 依次输入或选择各项参数
   - 3G功能：只有启动本功能后，才会触发3G拨号。
   - 用户名：拨号使用的用户名。
   - 密码：拨号使用的密码。
   - 拨号串：拨号使用的拨号串。TD-SCDMA、WCDMA的拨号串是*99#，CDMA2000的拨号串是#777
   - 在线方式：当用户是包月用户或者按流量计费的用户时选择“一直在线”方式。当用户是按时计费的用户时请选择“空闲自动断线”方式。在“空闲自动断线（秒）”内如果没有流量通过，则断开互联网的访问。
3. 单击“应用”。



总结

- VLAN的基本技术
- WLAN的基本技术
- SA、E1、ADSL、3G技术



思考题

- VLAN有哪些接口类型？各接口类型对Tag是如何处理？
- WLAN配置主要由哪些关键步骤组成？
- 什么是E1？
- 什么是SA？
- ADSL的上行和下行是什么意思？
- 3G配置主要由哪些关键步骤组成？



Thank you

www.huawei.com

HC110310008

HCNA-Security-CBSN 第八章 VPN 技术简介

第八章

VPN技术简介

www.huawei.com

HUAWEI



目标

- 学完本课程后，您将能够:
  - 了解VPN概念
  - 了解VPN有哪些关键技术
  - 了解VPN分类及应用
  - 了解L2TP基本原理知识及基本配置方法
  - 掌握GRE VPN的基本原理及配置方法





目录



VPN定义

- **VPN**

  虚拟专用网(Virtual Private Network)是一种“通过共享的公共网络建立私有的数据通道，将各个需要接入这张虚拟网的网络或终端通过通道连接起来，构成一个专用的、具有一定安全性和服务质量保证的网络”。

- **虚拟**

  用户不再需要拥有实际的专用长途数据线路，而是利用Internet的长途数据线路建立自己的私有网络。

- **专用网络**

  用户可以为自己制定一个最符合自己需求的网络。

 Page 3

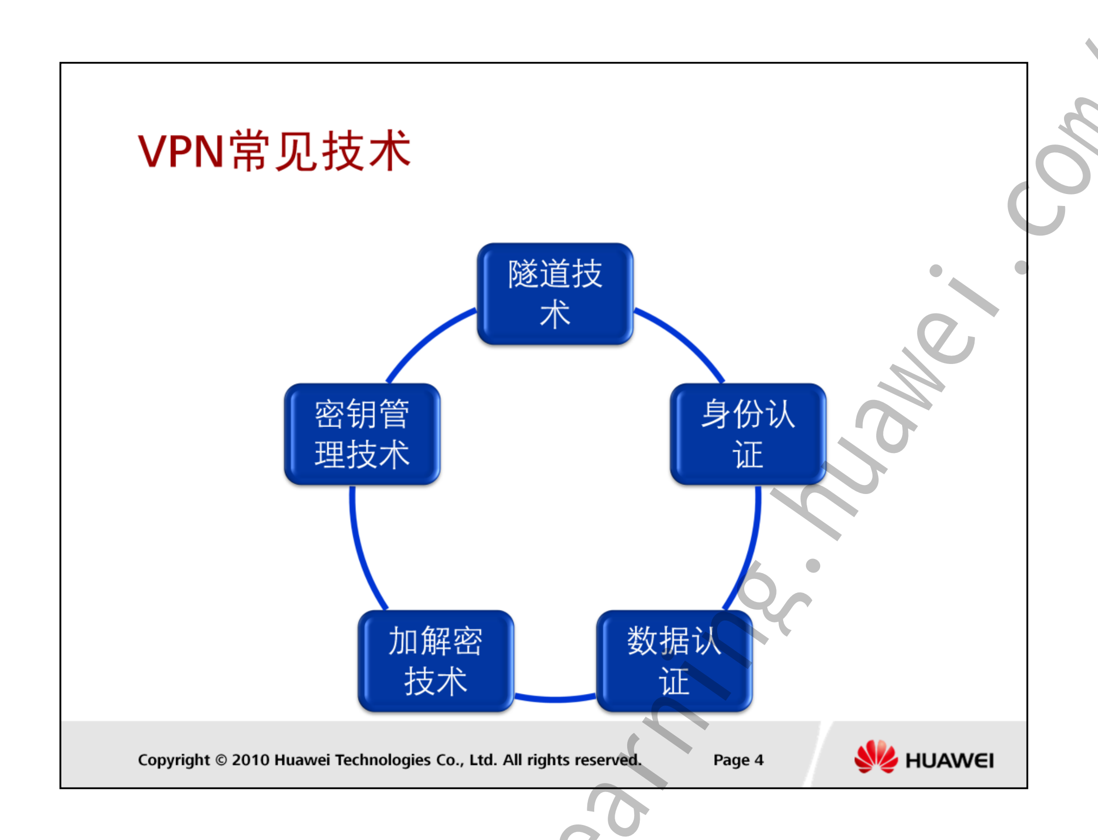


虚拟专用网（VPN）是指通过共享的公共网络建立私有的数据通道，将各个需要接入虚拟网的网络或终端通过通道连接起来，构成一个专用的、具有一定安全性和服务质量保证的网络。

传统的VPN组网主要采用专线VPN和基于客户端设备的加密VPN两种方式。专线VPN是指用户租用数字数据网（DDN）电路、ATM永久性虚电路（PVC）、帧中继（FR）PVC等组建一个二层的VPN网络，骨干网络由电信运营商进行维护，客户负责管理自身的站点和路由。基于客户端设备的加密VPN则将VPN的功能全部由客户端设备来实现，VPN各成员之间通过非信任的公网实现互联。第一种方式的成本比较高，扩展性也不好；第二种方式对用户端设备及人员的要求较高。

IETF草案对基于IP的VPN的理解是：“使用IP机制仿真出一个私有的广域网”。即通过隧道技术在公共数据网络上模拟出一条点到点的专线技术。所谓虚拟，是指用户不再需要拥有实际的专用长途数据线路，而是利用Internet的长途数据线路建立自己的私有网络。所谓专用网络，则是指用户可以为自己制定一个最符合自己需求的网络。

随着IP数据通信技术的不断发展，基于IP的VPN技术逐渐成为VPN市场的主流。由于IP VPN采用IP网络来承载，而且运营商网络越来越完善，因此成本较低，服务质量也足以满足客户需求，并且具有较好的可扩展性和可管理性。也正是如此，越来越多的用户开始选择IP VPN，运营商也建设IP VPN来吸引更多的用户。



VPN主要通过隧道技术来实现业务交付，但是由于公网上业务复杂，安全性较差，因此VPN还需采取其他技术保证数据的安全性，主要包括加解密技术、密钥管理技术、 数据认证技术和身份认证技术等。

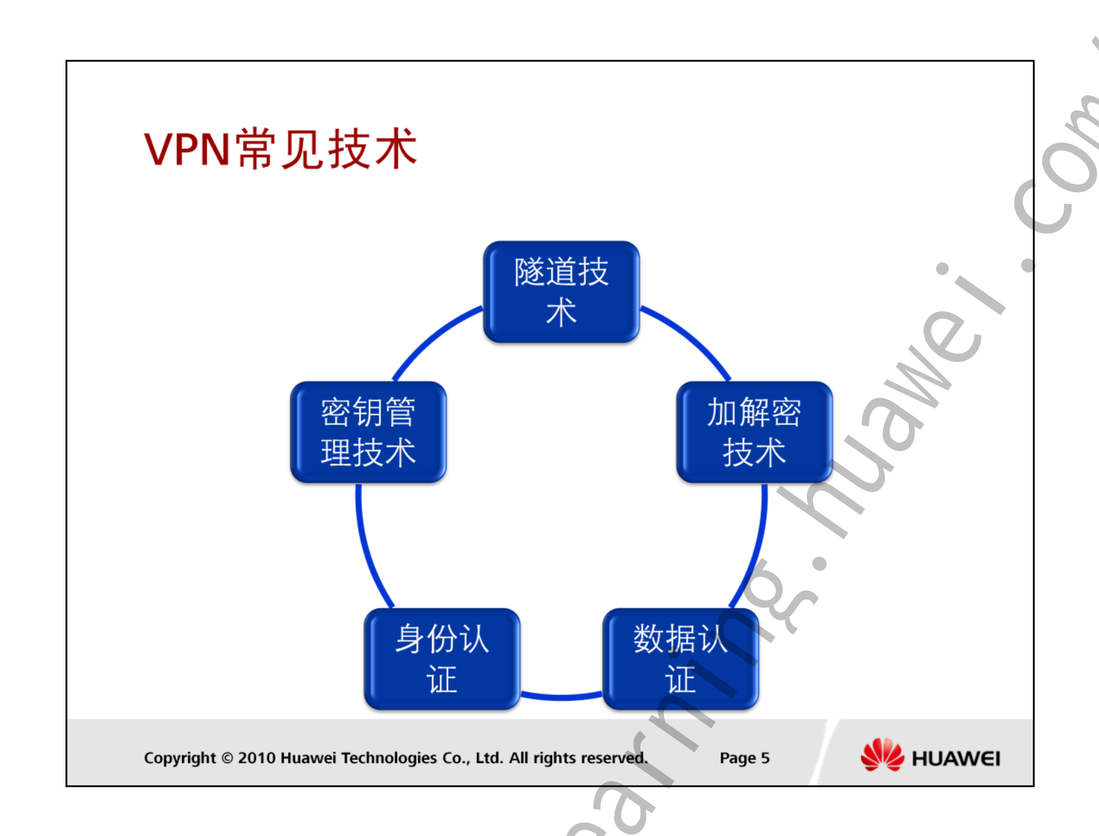
- 隧道技术

隧道技术是VPN技术中最关键的技术。隧道技术是指在隧道的两端通过封装以及解封装技术在公网上建立一条数据通道，使用这条通道对数据报文进行传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。二层隧道协议，使用二层网络协议进行传输，它主要应用于构建远程访问虚拟专网，第二层隧道协议主要有L2F、PPTP、L2TP等。L2TP协议是目前IETF的标准，由IETF融合PPTP与L2F而形成；三层隧道协议，用于传输三层网络协议，它主要应用于构建企业内部虚拟专网和扩展的企业内部虚拟专网，主要的第三层隧道协议有VTP、IPSec等。IPSec（IP Security）由多个协议组成，并通过这个协议集来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在IP层提供安全保障。

- 数据认证技术和身份认证技术

数据认证技术主要保证数据在网络传输过程中不被非法篡改。数据认证技术主要采用哈希算法，由于哈希算法的不可逆特性以及理论上的结果唯一性，因此在摘要相同的情况下可以保证数据没被篡改过。

身份认证技术主要保证接入VPN的操作人员的合法性以及有效性，主要采用“用户名密码”方式进行认证，对安全性较高的还可以使用USB KEY等认证方式。

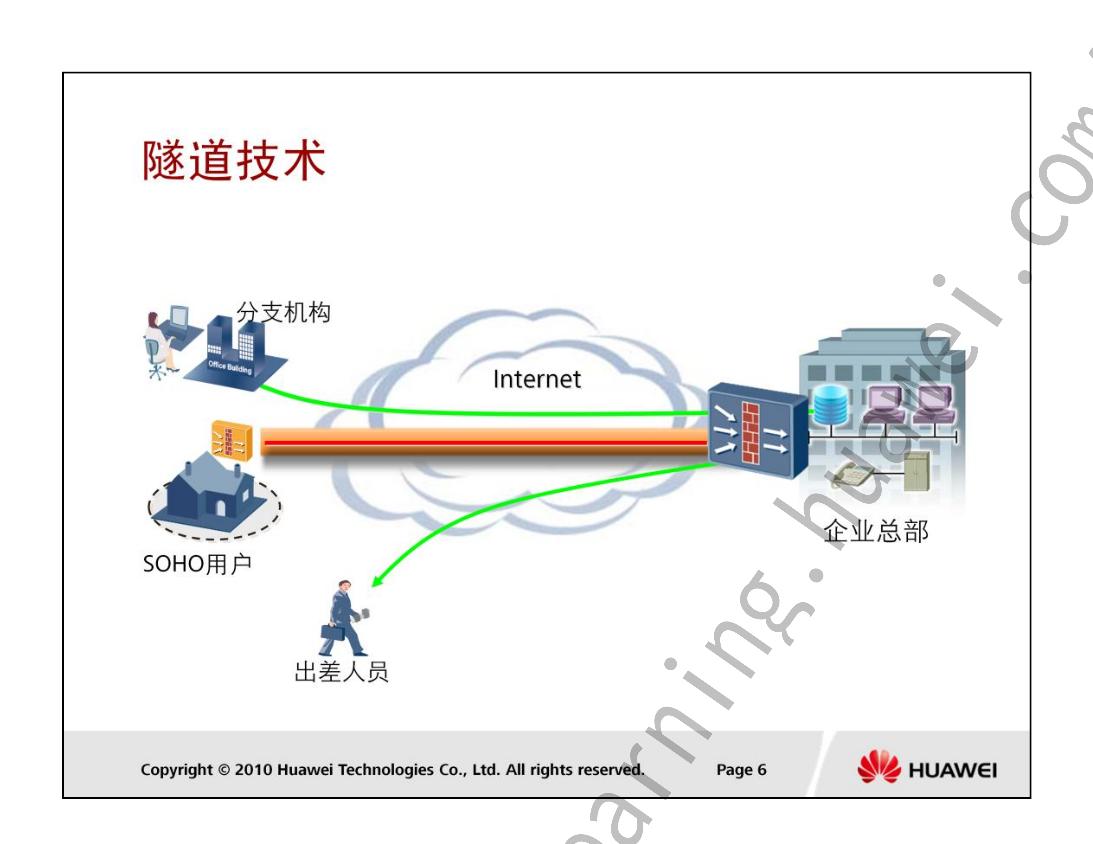


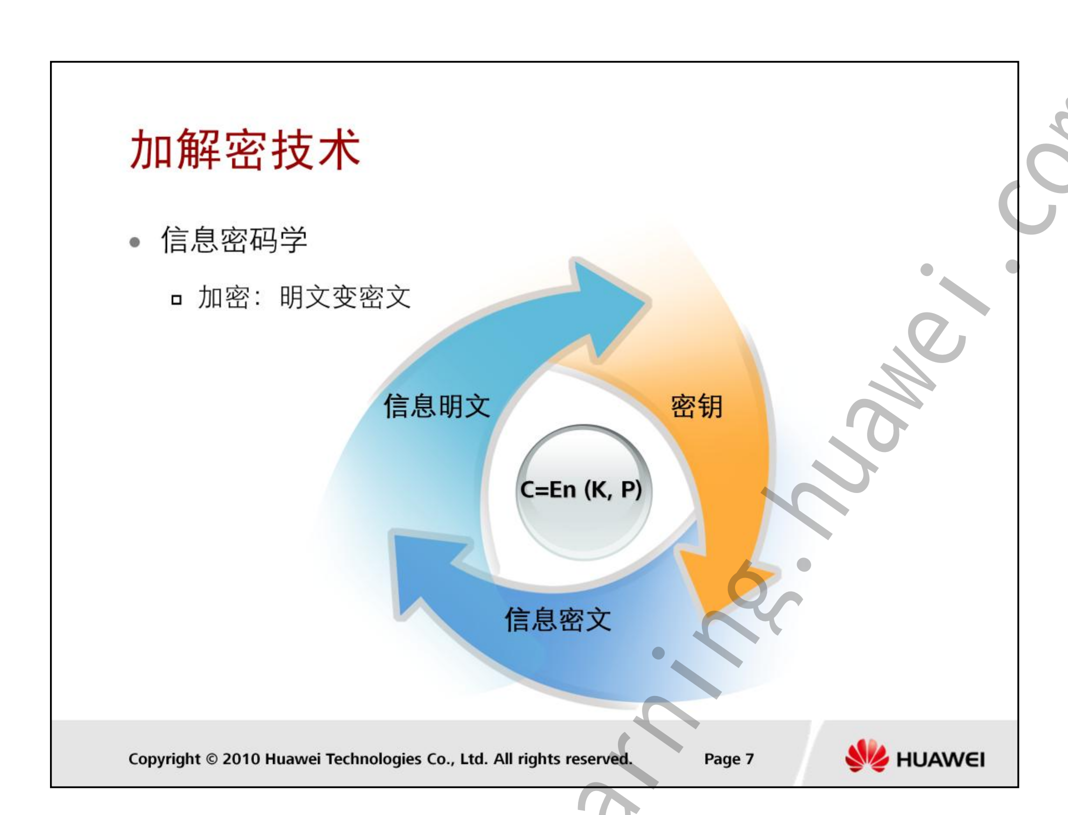
- 加解密技术

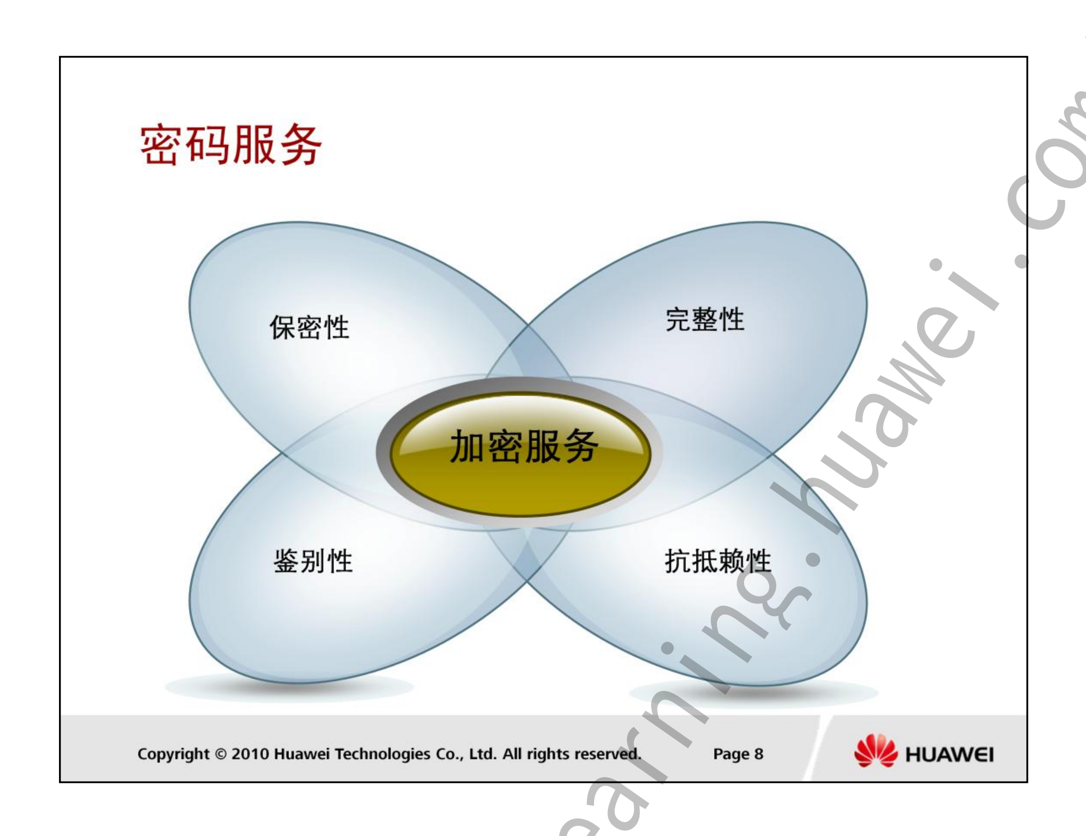
加解密技术是数据通信中一项较成熟的技术，VPN技术可以借助加解密技术保证数据在网络中传输时不被非法获取。即当数据被封装入隧道后立即进行加密，只有当数据到达隧道对端后，才能由隧道对端对数据进行解密。

- 密钥管理技术

密钥管理技术再VPN中的主要任务是在不安全的公用数据网上安全地传递密钥而不被窃取。最典型的应用就是IKE技术，IKE技术主要被IPSec VPN所借用，具体原理将在随后章节进行介绍。


隧道技术
分支机构
Office Building
Internet
SOHO用户
企业总部
出差人员
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 6
HUAWEI


加解密技术
信息密码学
加密：明文变密文
信息明文
密钥
C=En (K, P)
信息密文
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 7
HUAWEI



加密是一个过程，它使信息只对正确的接收者可读，其他用户看到的是杂乱无序的信息，使其只能在使用相应的密钥解密之后才能显示出本来内容。通过加密的方法来达到保护数据不被非法人窃取、阅读的目的。加密在网络上的作用就是防止私有化信息在网络上被拦截和窃取。一个简单的例子就是密码的传输，计算机密码极为重要，许多安全防护体系是基于密码的，密码的泄露在某种意义上来讲意味着其安全体系的全面崩溃。

因此密码提供的服务也是信息安全的服务要求：

- 机密性：通过数据加密实现

提供只允许特定用户访问和阅读信息，任何非授权用户对信息都不可理解的服务。这是使用加密的普遍原因。通过小心使用数学方程式，可以保证只有对应接收人才能查看它

- 完整性：通过数据加密、散列或数字签名来实现

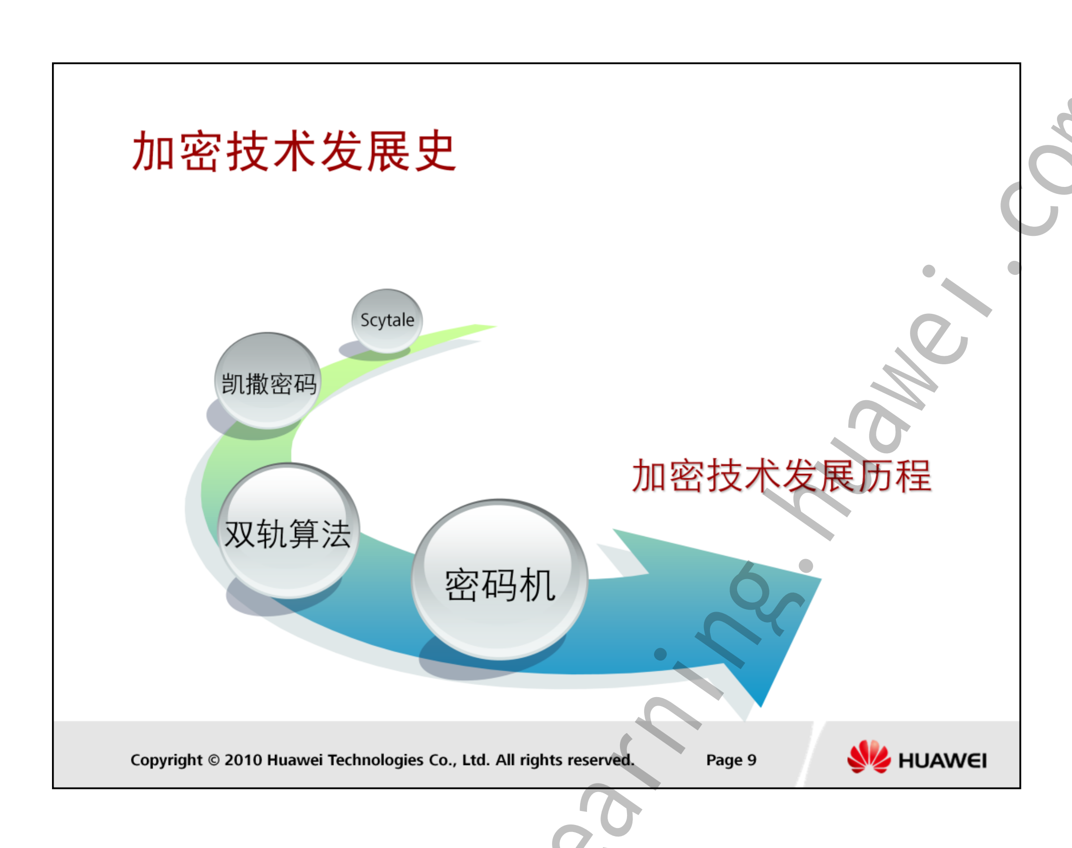
提供确保数据在存储和传输过程中不被未授权修改（篡改、删除、插入和重放等）的服务。对安全级别需求较高的用户来说，仅仅数据加密是不够的，数据仍能够被非法破解并修改。

- 鉴别性：通过数据加密、数据散列或数字签名来实现

提供与数据和身份识别有关的服务，即认证数据发送和接受者的身份。

- 不可否定性：通过对称加密或非对称加密，以及数字签名等，并借助可信的注册机构或证书机构的辅助来实现

提供阻止用户否认先前的言论或行为的抗抵赖服务。



加密作为保障信息安全的一种方式，它不是现代才有的，它产生的历史相当久远，可以追溯到人类刚刚出现，并且尝试去学习如何通信的时候。他们不得不去寻找方法确保他们的通信的机密。但是最先有意识地使用一些技术方法来加密信息的可能是公元六年前的古希腊人。他们使用的是一根叫scytale的棍子，送信人先绕棍子卷一张纸条，然后把要加密的信息写在上面，接着打开纸送给收信人。如果不知道棍子的宽度（这里作为密钥）是不可能解密信里面内容的。

大约在公元前50年，古罗马的统治者凯撒发明了一种战争时用于传递加密信息的方法，后来称之为“凯撒密码”。它的原理就是：将26个字母按自然顺序排列，并且首尾相连，明文中的每个字母都用其后的第三个字母代替，例如HuaweiSymantec通过加密之后就变成KxdzhlvBPdqwhf。

近期加密技术主要应用于军事领域，如美国独立战争、美国内战和两次世界大战。在美国独立战争时期，曾经使用过一种“双轨”密码，就是先将明文写成双轨的形式，然后按行顺序书写。在第一次世界大战中，德国人曾依靠字典编写密码，比如：10-4-2，就是某字典第10页，第4段的第2个单词。在二次世界大战中，最广为人知的编码机器是德国人的Enigma三转轮密码机，在二次世界大战中德国人利用它加密信息。

20世纪，美国人对计算机的研究就是为了破解德国人的密码，当时的人们并没有想到计算机给今天带来的信息革命。随着计算机的发展，运算能力的增强，传统密码的破解变得十分简单了，同时随着计算机在商业、个人等领域的不断扩展，使得商业或个人对数据保护、数据传输的安全性、防止信息数据泄露越来越重视，正是因为这些原因大大促进了加密技术的发展，美国人提出了公钥加密体系，从而使加密技术进入一个全新的发展阶段。

加密技术分类

- **对称加密**
  - 加密、解密用同一个密钥
- **非对称加密**
  - 在加密和解密中使用两个不同的密钥，私钥用来保护数据，公钥则由同一系统的人公用，用来检验信息及其发送者的真实性和身份。
  - 密钥
    - 私钥
    - 公钥

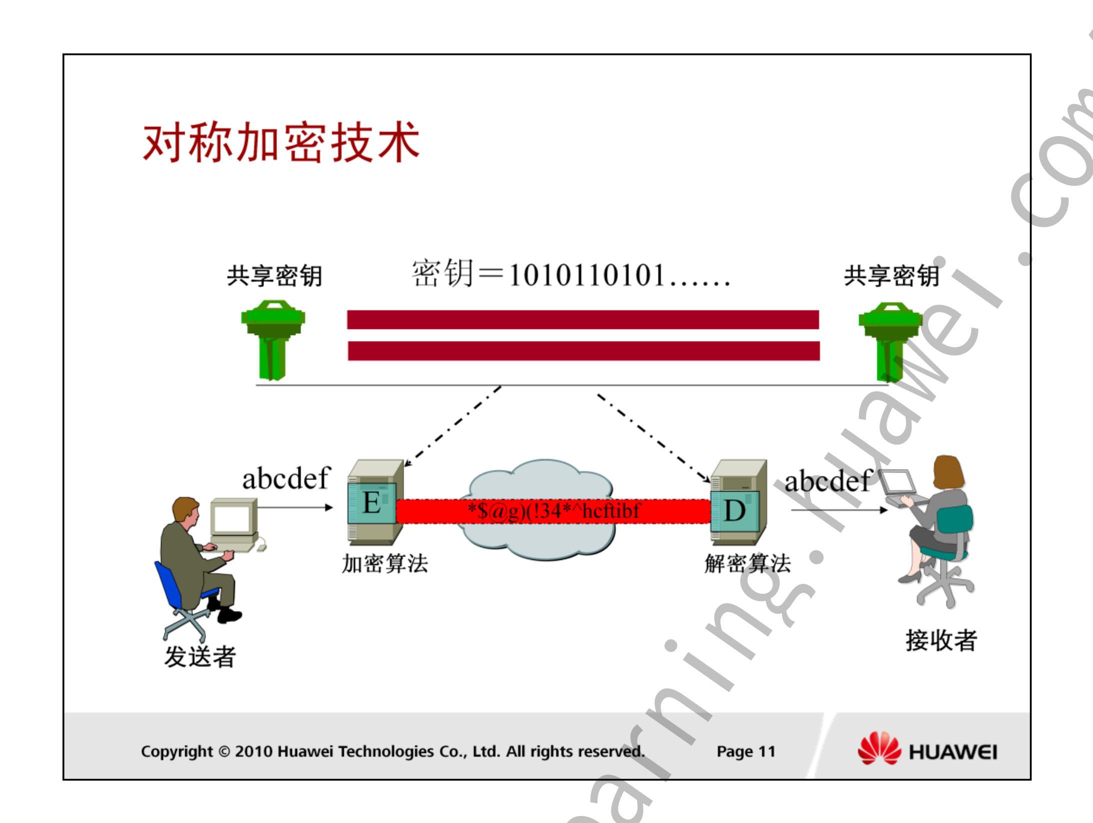
 Page 10 

对称加密算法也叫传统密码算法（秘密密钥算法、单钥算法），加密密钥能从解密密钥中推算出来。发件人和收件人共同拥有同一个密钥，既用于加密也用于解密。对称密钥加密是加密大量数据的一种行之有效的方法。对称密钥加密有许多种算法，但所有这些算法都有一个共同的目的：以可以还原的方式将明文（未加密的数据）转换为暗文。由于对称密钥加密在加密和解密时使用相同的密钥，所以这种加密过程的安全性取决于是否有未经授权的人获得了对称密钥。特别注意：希望使用对称密钥加密通信的双方，在交换加密数据之前必须先安全地交换密钥。

衡量对称算法优劣的主要尺度是其密钥的长度。密钥越长，在找到解密数据所需的正确密钥之前必须测试的密钥数量就越多。需要测试的密钥越多，破解这种算法就越困难。有了好的加密算法和足够长的密钥，如果有人想在一段实际可行的时间内逆转转换过程，从暗文中推导出明文，从应用的角度来讲，这种做法是徒劳的。

非对称算法也叫公钥加密，使用两个密钥：一个公钥和一个私钥，这两个密钥在数学上是相关的。在公钥加密中，公钥可在通信双方之间公开传递，或在公用储备库中发布，但相关的私钥是保密的。只有使用私钥才能解密用公钥加密的数据。使用私钥加密的数据只能用公钥解密。与对称密钥加密相似，公钥加密也有许多种算法。然而，对称密钥和公钥算法在设计上并无相似之处。您可以在程序内部使用一种对称算法替换另一种，而变化却不大，因为它们的工作方式是相同的。而不同公钥算法的工作方式却完全不同，因此它们不可互换。

公钥算法是复杂的数学方程式，使用十分大的数字。公钥算法的主要局限在于，这种加密形式的速度相对较低。实际上，通常仅在关键时刻才使用公钥算法，如在实体之间交换对称密钥时，或者在签署一封邮件的散列时（散列是通过应用一种单向数学函数获得的一个定长结果，对于数据而言，叫做散列算法）。



- 对称密钥算法体系包括：
  - 明文(plaintext)：这是原始消息或数据，作为算法的输入。
  - 加密算法(encryption algorithm)：加密算法对明文进行各种替换和转换。
  - 秘密密钥(secret key)：秘密密钥也是算法的输入。算法进行的具体替换和转换取决于这个密钥。
  - 密文(ciphertext)：这是产生的已被打乱的消息输出。它取决于明文和秘密密钥。对于一个给定的消息，两个不同的密钥会产生两个不同的密文。
  - 解密算法(decryption algorithm)：本质上是加密算法的反向执行。它使用密文和同一密钥产生原始明文。
- 加解密过程如下：

  1、发送者用密钥K将明文X加密为Y，这个过程表示为Y=E[K,X]。

  2、接收者用密钥K将密文Y解密为X，这个过程表示为X=D[K,Y]。
- 对称加密的安全使用有两个要求：

  1、需要一个强（strong）加密算法。这个要求简单地说就是：密钥要足够强壮，使得攻击者不能通过已有的明文和密文对应来破解。

  2、密钥的传递需要一个安全的方式。也就是要求发送者要把密钥通过安全的方式告诉接收者，不能让第三方知道。

常见的对称加密算法

- 流加密算法
  - RC4
- 分组加密算法
  - DES
  - 3DES
  - AES
  - IDEA
  - RC2，RC5，RC6



有很多特殊的数学算法来实现对称加密，主要包括两类：

- 流加密算法（stream algorithm）

流加密算法在算法过程中连续输入元素，一次产生一个输出元素。典型的流密码算法一次加密一个字节的明文，密钥输入到一个伪随机字节生成器，产生一个表面随机的字节流，称为密钥流。流加密算法一般用在数据通信信道，浏览器或网络链路上常见的流加密算法：RC4是Ron Rivest在1987年为RSA Security公司设计的流加密算法。它是密钥大小可变的流密码，使用面向字节的操作，就是实时的把信息加密成一个整体。

- 分组算法（block algorithm）

分组加密算法的输入为明文分组及密钥，明文被分为两半，这两半数据通过n轮处理后组合成密文分组，每轮的输入为上轮的输出；同时子密钥也是由密钥产生。典型分组长度是64位。分组算法包括以下几种：

  - 数据加密标准（DES， Data Encryption Standard）

DES是第一个得到广泛应用的密码算法，使用相同的密钥来加密和解密。DES是一种分组加密算法，输入的明文为64位，密钥为56位，生成的密文为64位（把数据加密成64位的block）。

  - 三重数据加密标准（3DES， Triple DES）

3DES使用了128位密钥。信息首先使用56位的密钥加密，然后用另一个56位的密钥译码，最后再用原始的56位密钥加密，这样3DES使用了有效的128位长度的密钥。Triple DES最大的优点就是可以使用已存在的软件和硬件，并且在DES加密算法上的技术可以轻松的实施Triple DES。

常见的对称加密算法

- 流加密算法
  - RC4
- 分组加密算法
  - DES
  - 3DES
  - AES
  - IDEA
  - RC2，RC5，RC6

 Page 13 

- 高级加密标准（AES，Advanced Encryption Standard）

AES采用128位的分组长度，支持长度为128位、192位和256位的密钥长度，并可支持不同的平台。128位的密钥长度能够提供足够的安全性，而且比更长的密钥需要较少的处理时间。到目前为止，AES还没有出现任何致命缺陷。AES取代DES和3DES以增强安全性和效率已是大势所趋。

- IDEA（International Data Encryption Algorithm）

IDEA是对称分组密码算法，输入明文为64位，密钥为128位，生成的密文为64位。

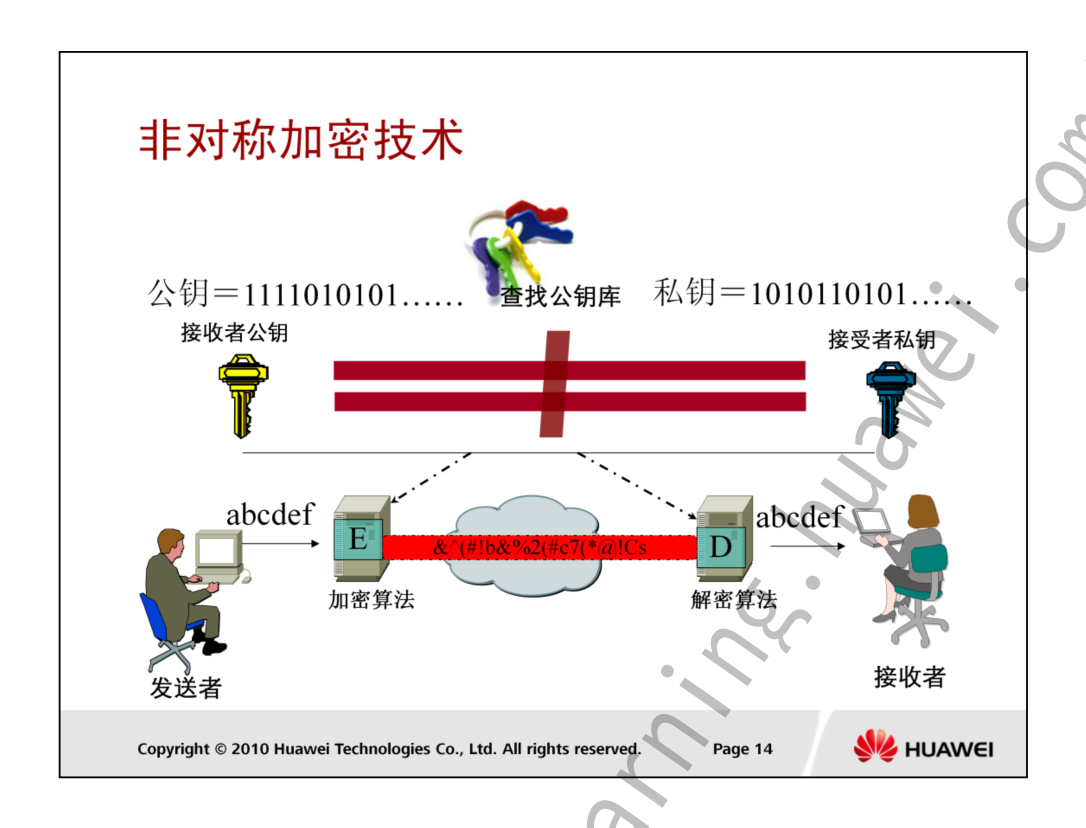
- RC2，RC5，RC6

RC2是Ron Rivest为RSA公司设计的变长密钥加密算法，它是一种block模式的密文，就是把信息加密成64位的数据。因为它可以使用不同长度的密钥，它的密钥长度可以从零到无限大，并且加密的速度依赖于密钥的大小。

RC5是由RSA公司的Rivest于1994年设计的一种新型的分组密码算法。RC5类似于RC2，也是block密文，但是这种算法采用不同的block大小和密钥大小。另外此算法中数据所通过的round也是不同的。一般建议使用128位密钥的RC5算法，并运行12到16个rounds。它是一种分组长度、密钥长度和迭代轮数都可变的分组迭代密码算法。

RC6不像其它一些较新的加密算法，RC6包括整个算法的家族。RC6系列在1998年被提出在RC5算法提出来后，经调查发现其在对特殊的round上加密时存在于一个理论上的漏洞。RC6的设计弥补了这种漏洞。

常用的分组对称加密算法是：DES，3DES，AES。

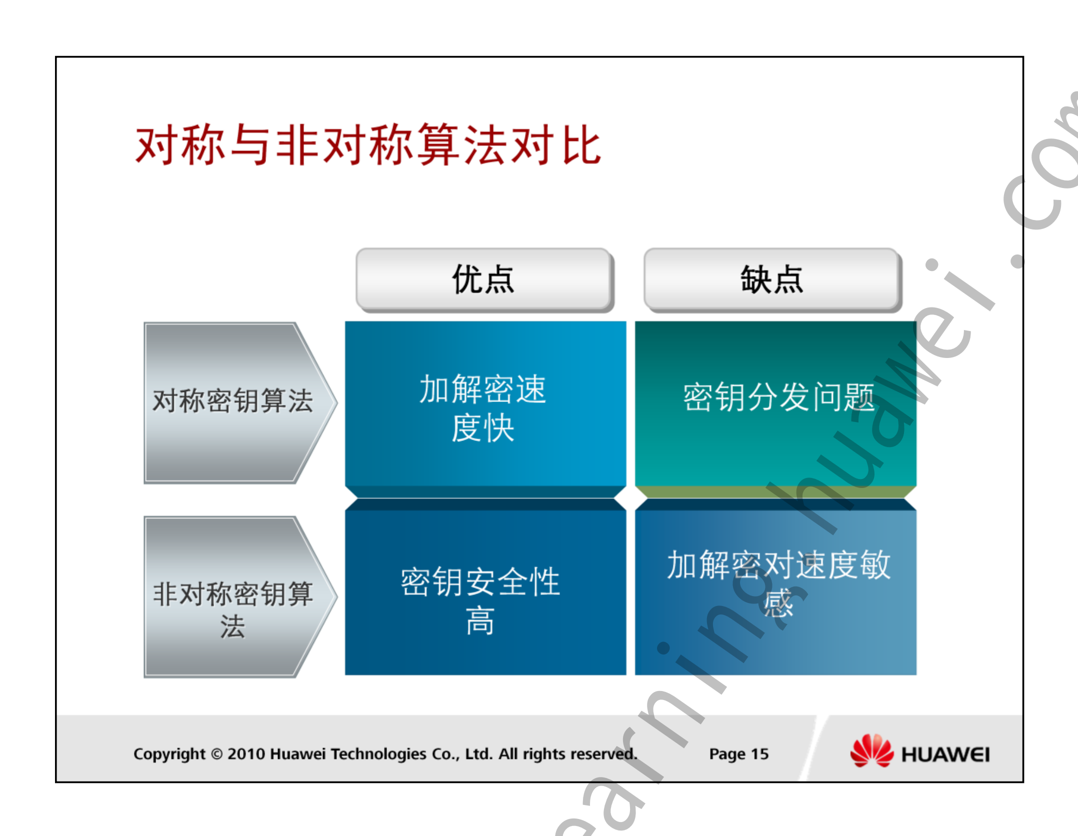


非对称加密使用两个密钥：一个公钥和一个私钥，这两个密钥在数学上是相关的。公钥可在通信双方之间公开传递，或在公用储备库中发布，但相关的私钥是保密的。只有使用私钥才能解密用公钥加密的数据，使用私钥加密的数据只能用公钥解密。非对称密钥算法体系包括：

- 明文：它是可读的消息或者数据，用作算法的输入。
- 加密算法：加密算法对明文进行各种形式的变换。
- 公钥和私钥：它们是被选择的一对密钥，如果一个密钥用于加密，则另一个密钥用作解密。其中公钥是公开给其他人的，私钥是只有自己知道的。
- 密文：它是输出的混乱的消息，取决于明文和密钥。
- 解密算法：该算法接受密文和匹配的密钥，生成原始的明文。

非对称算法加解密的基本步骤如下：

1. 每个用户都生成一对密钥。
2. 每个用户都把其中一个密钥放在一个公用的寄存器或者可访问的文件夹里，作为公钥，剩下一个自己保存为私钥。每个用户都保存着别人的公钥。
3. 如图，如果甲要给接收者发送消息，则发送者在自己或者公共的公钥库里找出接收者的公钥PU，用之来将消息X转换为密文Y，这个过程表示为Y=E[PU，X]然后将密文发送给接收者。
4. 接收者收到密文Y后，用自己的私钥PR来将接收到的密文Y解密为明文消息X。这个过程表示为X=D[PR，Y]，私钥只有接收者拥有，所以别人不能将密文解密。



- 对称密钥算法

1、对称密钥的主要优点在于速度快，通常比非对称密钥快100倍以上，而且可以方便地通过硬件实现。

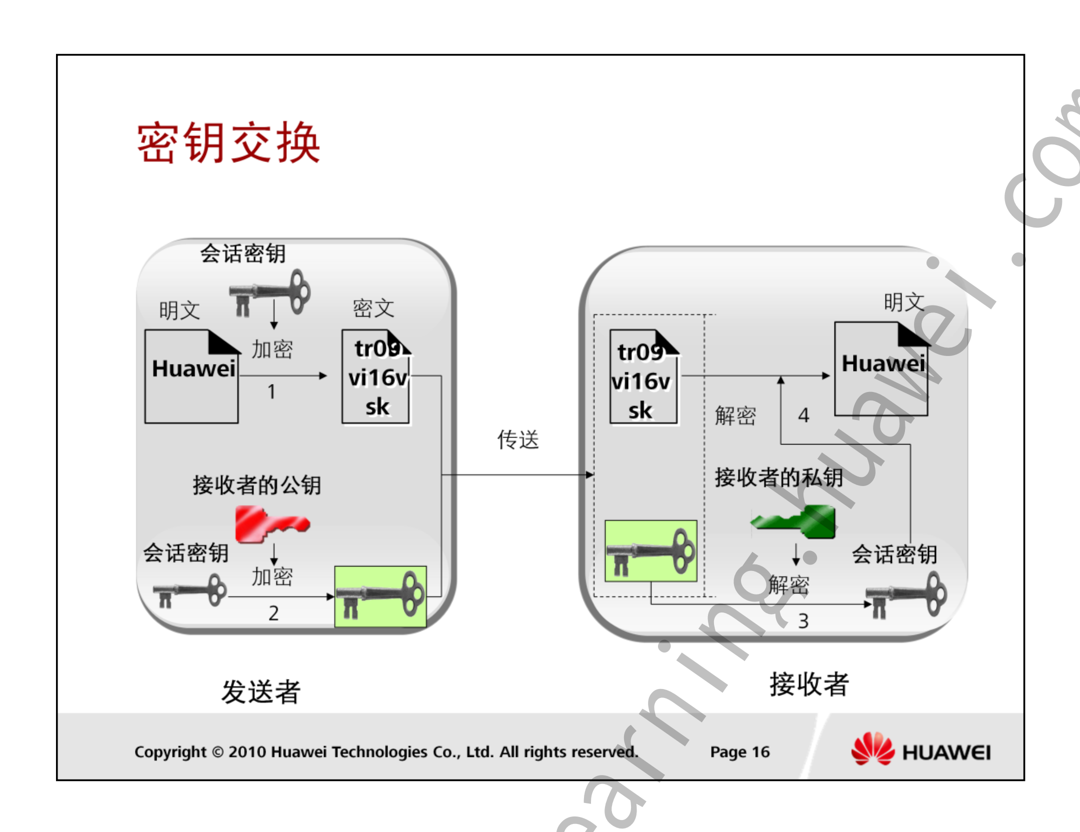
2、主要问题在于密钥的管理复杂。由于每对通信者间都需要一个不同的密钥，N个人通信需要 = n(n-1)/2密钥；同时如何安全的共享秘密密钥给需要解密的接受者成为最大的问题；并且由于没有签名机制因此也不能实现抗可抵赖问题，即通信双方都可以否认发送或接收过的信息。

- 非对称密钥算法

1、非对称密钥的主要优势在于密钥能够公开，由于用作加密的密钥（也称公开密钥）不同于用作解密的密钥（也称私人密钥)，因而解密密钥不能根据加密密钥推算出来，所以可以公开加密密钥。公钥加密提供了一种有效的方法，可用来把为大量数据执行对称加密时使用的机密密钥发送给某人。私钥加密而用公钥解密，主要用于数字签名。

2、主要局限就是速度。实际上，通常仅在关键时刻才使用公钥算法，如在实体之间交换对称密钥时，或者在签署一封邮件的散列时（散列是通过应用一种单向数学函数获得的一个定长结果，对于数据而言，叫做散列算法）。

对称和非对称密钥算法通常结合使用，用于密钥加密和数字签名，即实现安全又能优化性能。



- 密钥交换：结合使用对称与非对称密钥

对称密钥算法非常适合于快速并安全地加密数据。但缺点是，发件人和收件人必须在交换数据之前先交换机密密钥。结合使用加密数据的对称密钥算法与交换机密密钥的公钥算法可产生一种既快速又灵活的解决方案。

- 基于公钥的密钥交换步骤如下：

1、发件人获得收件人的公钥；

2、发件人创建一个随机机密密钥（在对称密钥加密中使用的单个密钥）；

3、发件人使用机密密钥和对称密钥算法将明文数据转换为暗文数据；

4、发件人使用收件人的公钥将机密密钥转换为暗文机密密钥；

5、发件人将暗文数据和暗文机密密钥一起发给收件人；

6、收件人使用其私钥将暗文机密密钥转换为明文；

7、收件人使用明文机密密钥将暗文数据转换为明文数据。

- 其特点在于：

1、产生一个一次性对称密钥—会话密钥；

2、用会话密钥加密信息；

3、最后用接收者的公钥加密会话密钥—因为它很短，加解密迅速。

数据认证--散列算法

- 散列算法：把任意长度的输入变换成固定长度的输出
  - h=H(M)
- 常见散列算法
  - MD5
  - SHA-1

 Page 17 

- 散列算法加密原理

在通讯的过程中，数据发送方通常对传输的数据进行HASH计算得到一个HASH值，并对该HASH值进行加密，并将其与数据一同发送出去，接收方收到数据后对数据进行HASH计算，并比较收到的HASH值，如果相同则表示数据没有损坏或被篡改。

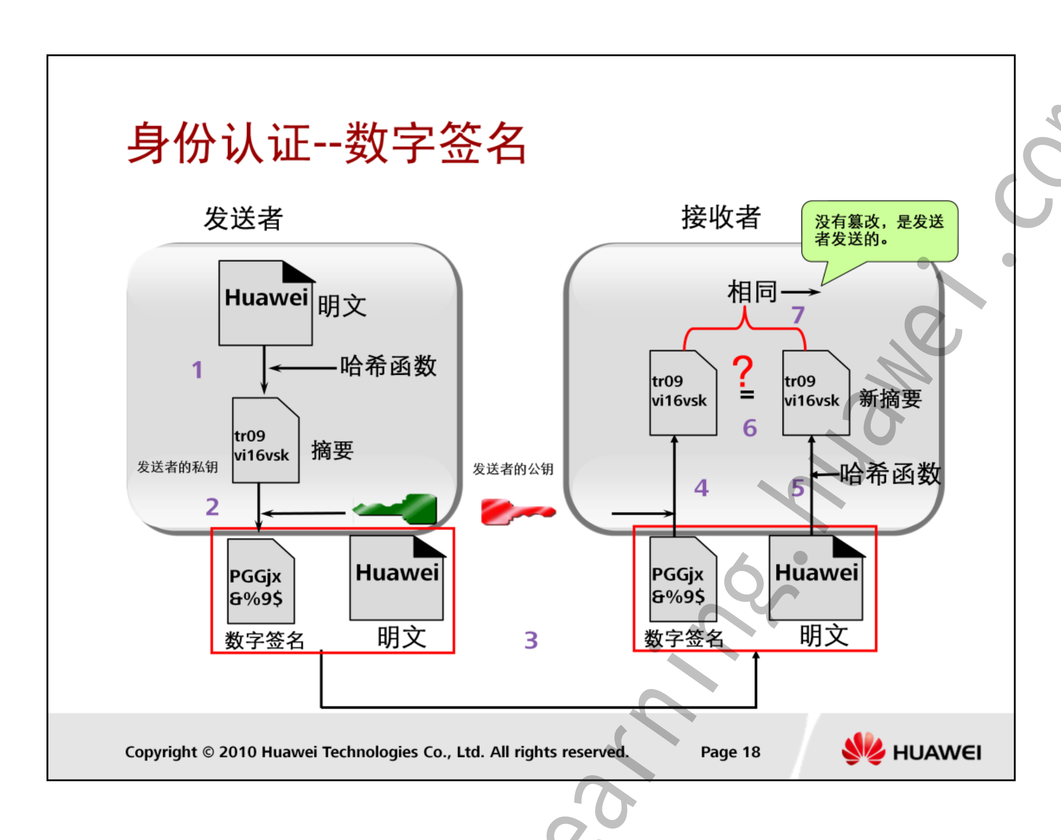
哈希加密是通信的双方通过对比各自的哈希值，从而判断信息是否变更的方法，这可以运用在信息完整性的验证中。哈希加密的另外一种用途是签名文件。

- 信息 – 摘要算法（MD5，Message-DigestAlgorithm5）

MD5是由MD2、MD3、MD4发展而来的一种单向函数算法（也就是HASH算法），可产生一个128位的散列值。它是国际著名的公钥加密算法标准RSA的第一设计者R.Rivest于上个世纪90年代初开发出来的。MD5的最大作用在于，将不同格式的大容量文件信息在用数字签名软件来签署私人密钥前“压缩”成一种保密的格式，关键之处在于这种“压缩”是不可逆的。MD5设计经过优化以用于Intel处理器。这种算法的基本原理已经泄露，这就是为什么它不太受欢迎的原因。

- SHA-1

SHA-1是流行的用于创建数字签名的单向散列算法。与DSA公钥算法相似，安全散列算法1（SHA-1）也是由NSA设计的，并由NIST将其收录到FIPS中，作为散列数据的标准。它可以将任意长度的字符串计算为160位的HASH值。SHA在结构上类似于MD4和MD5。尽管它比MD5的速度要慢25%，但它更加安全。它产生的信息摘要比MD5要长25%，因此对于攻击来说是更安全的。不过鉴于SHA-1的漏洞也被发现，于2010年前逐步推广更安全的SHA-224、SHA-256、SHA-384和SHA-512。



数字签名主要的功能是：保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名，包括普通数字签名和特殊数字签名。普通数字签名算法有RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir数字签名算法、Des/DSA，椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等。数字签名技术是公钥密码体制的典型应用。数字签名的应用过程是，数据源发送方使用自己的私钥对数据校验和或其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”，数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。在数字签名应用中，发送者的公钥可以很方便地得到，但他的私钥则需要严格保密。数字签名可用作数据完整性检查并提供拥有私钥的凭据，签署和验证数据的步骤如下：

1. 发送者将一种散列算法应用于数据，并生成一个散列值；
2. 发送者使用私钥将散列值转换为数字签名；
3. 发送者将数据、签名发给接收者；
4. 接收者使用发送者的公钥对数字前面进行解密；
5. 发送者将该散列算法应用于接收到的数据，并生成一个散列值；
6. 比较发送者发送的散列值与新生成的散列值是否相同。
7. 散列值相同则表示该消息来自与发送者，并且消息未被篡改。

身份认证--数字证书

- 公钥的载体
- 数字证书的格式X.509
- 由受信任的机构颁发
- 数字证书的存储



 Page 19 HUAWEI

数字证书由三部分组成：主体部分、算法部分和签名部分。其中主体部分包括：

- 证书格式版本（version）：版本号指明X.509证书的格式版本，现在的值可以为v1（0），v2（1），v3（2）。
- 证书序列号（Serial Number）：序列号指定由CA分配给证书的唯一的数字型标识符。当证书被取消时，实际上是将此证书的序列号放入由CA签发的CRL中，这也是序列号唯一的原因。
- 签名算法标识（Signature）：签名算法标识用来指定由CA签发证书时所使用的签名算法。算法标识符用来指定CA签发证书时所使用的公开密钥算法和Hash算法，须向国际知名标准组织（如ISO）注册。
- 签发CA名称（Issuer）：此域用来标识签发证书的CA的X.509DN名字。包括国家、省市、地区、组织机构、单位部门和通用名。
- 证书有效期（Validity）：指定证书的有效期，包括证书开始生效的日期和时间以及失效的日期和时间。每次使用证书时，需要检查证书是否在有效期内。
- 证书持有者名称（Subject）：指定证书持有者的X.509唯一名字。包括国家、省市、地区、组织机构、单位部门和通用名，还可包含email地址等个人信息等
- 证书公钥（Subject Public Key Info）：证书持有者公开密钥信息域包含两个重要信息：证书持有者的公开密钥的值；公开密钥使用的算法标识符。此标识符包含公开密钥算法和hash算法。

身份认证--数字证书

- 公钥的载体
- 数字证书的格式X.509
- 由受信任的机构颁发
- 数字证书的存储



 Page 20 HUAWEI

- 证书废除列表证书黑名单（CRL， Certificate Revocation Lists）：为应用程序和其它系统提供了一种检验证书有效性的方式。任何一个证书废除以后，证书机构CA会通过发布CRL的方式来通知各个相关方。

数字证书作为一种电子数据格式，可以直接从网上下载，也可以通过其他方式。使用IC卡存放用户证书，即把用户的数字证书写到IC卡中，供用户随身携带。这样用户在所有能够读IC卡证书的电子商务终端上都可以享受安全电子商务服务。用户证书直接存放在磁盘或自己的终端上。户将从CA申请来的证书下载或复制到磁盘或自己的PC机或智能终端上，当用户使用自己的终端享受电子商务服务时，直接从终端读入即可。

密钥管理技术

- 密钥产生
- 分配保存
- 更换与销毁

 Page 21 

密钥管理是数据加密技术中的重要一环，密钥管理的目的是确保密钥的安全性（真实性和有效性）。为了数据使用的方便，数据加密在许多场合集中表现为密钥的应用，以达到保密的要求，因此密钥往往是保密与窃密的主要对象。密钥的管理技术包括密钥的产生、分配保存、更换与销毁等各环节上的保密措施。

- 密钥产生

层次化的密钥管理方式，用于数据加密的工作密钥需要动态产生；工作密钥由上层的加密密钥进行保护，最上层的密钥称为主密钥，是整个密钥管理系统的核心；多层密钥体制大大加强了密码系统的可靠性，因为用得最多的工作密钥常常更换，而高层密钥用的较少，使得破译者的难度增大。

- 分配保存

密钥的分配是指产生并使使用者获得一个密钥的过程；密钥的传递分集中传送和分散传送两类。集中传送是指将密钥整体传送，这时需要使用主密钥来保护会话密钥的传递，并通过安全渠道传递主密钥。分散传送是指将密钥分解成多个部分，用秘密分享的方法传递，只要有部分到达就可以恢复，这种方法适用于在不安全的信道中传输。

- 更换销毁

密钥既可以作为一个整体保存，也可以分散保存。整体保存的方法有人工记忆、外部记忆装置、密钥恢复、系统内部保存；分散保存的目的是尽量降低由于某个保管人或保管装置的问题而导致密钥的泄漏。密钥的备份可以采用和密钥的分散保存一样的方式，以免知道密钥的人太多；密钥的销毁要有管理和仲裁机制，否则密钥会被有意无意的丢失，从而造成对使用行为的否认。

密钥管理系统

- 一个完整的密钥管理系统应该做到：
  - 密钥难以被窃取和复制
  - 即使窃取了密钥也没有用，密钥有使用范围和时间的限制
  - 密钥的分配和更换过程对用户透明，用户不一定要亲自掌管密钥
  - 核心密钥一定要采用分割分责的方式保存



- 一个密钥管理系统应当基于共同的标准、程序和安全方法的集合，它们用于：
  - 为不同的密码系统和不同的应用软件生成密钥。
  - 生成和获取公共密钥证明。
  - 把密钥分发给需要的用户，包括接到密钥时应当怎样将其激活。
  - 存储密钥，包括经授权的用户怎样得到密钥。
  - 更改或者更新密钥，包括关于何时应该改变密钥和怎样改变的一些规则。
  - 处理受损的密钥。
  - 激活密钥，包括应当怎样将密钥撤出或者使其失效，例如密钥在何时被损害或者用户在何时离开了组织（在此种情况下密钥也应当被存档）。
  - 作为业务连续性管理的一部分，恢复丢失的或者毁坏的密钥。例如加密信息的恢复。
  - 存档密钥，例如用于信息存档或者备份。
  - 销毁密钥。
  - 密钥管理相关活动的记录和查验。

密钥管理策略

- 一个完整的密钥管理策略应该做到：
  - 密码策略控制是否允许用户重新使用旧的密码（强制密码历史），在两次更改密码之间的时间（最大密码寿命以及最小密码寿命），最小密码长度以及用户是否必须混合使用大小写字母、数字和特殊字符（密码必须满足复杂性要求）。
  - 帐户锁定策略确定了在特定时间段内锁定帐户之前，系统能够接受多少次失败的登录尝试
  - 法律要求和服务合同

 Page 23 

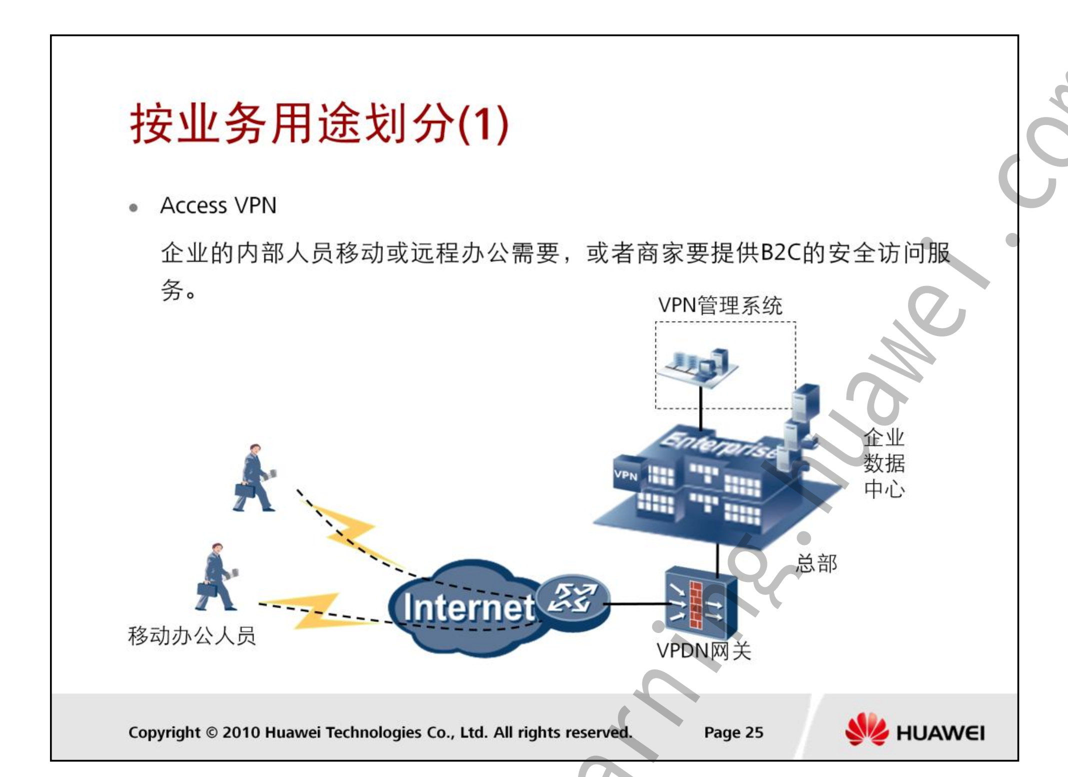
为了减少损害的可能性，密钥应当有确定的激活和休止日期，从而它们只能在有限的时间段内使用。该时间段的长度应当取决于运用密码管理措施的环境和所发现的风险。为了处理访问密码关键字的法律要求，需要考虑一些程序。例如，可能需要用加密信息的解密形式做法庭上的证据。服务等级管理的内容或者与外部密码服务供应商所签订合同的内容，例如与一个权威验证机构所签合同，应当包括有关责任、服务的可靠性和提供服务的响应时间等议题。参考经济合作与发展组织 (OECD, Organization for Economic Cooperation and Development)的密码政策：

- 为增强使用信息和通讯系统的信心，密码方法应当是可信赖的；
- 在法律许可范围内，用户可以自由选择密码方法；
- 密码方法的开发应适应个人、公司、政府的不同需求；
- 密码方法的标准、准则、协议的开发和颁布应在国家或国际范围内进行；
- 个人的基本隐私权，如通信秘密、个人数据保护，应在国家的密码政策及密码技术的实现和使用中得到尊重；
- 国家的密码政策应允许依法存取加密数据的明文或密钥，但这个政策应最大程度上不妨碍本指导原则中其它原则；
- 无论是采取立法或合约的形式，应明确提供密码服务或持有、存取密钥的个人或团体的责任；
- 政府在密码政策的制定中应协调各方面的关系，避免以密码政策的名义妨碍正常贸易或滥用法律。



目录





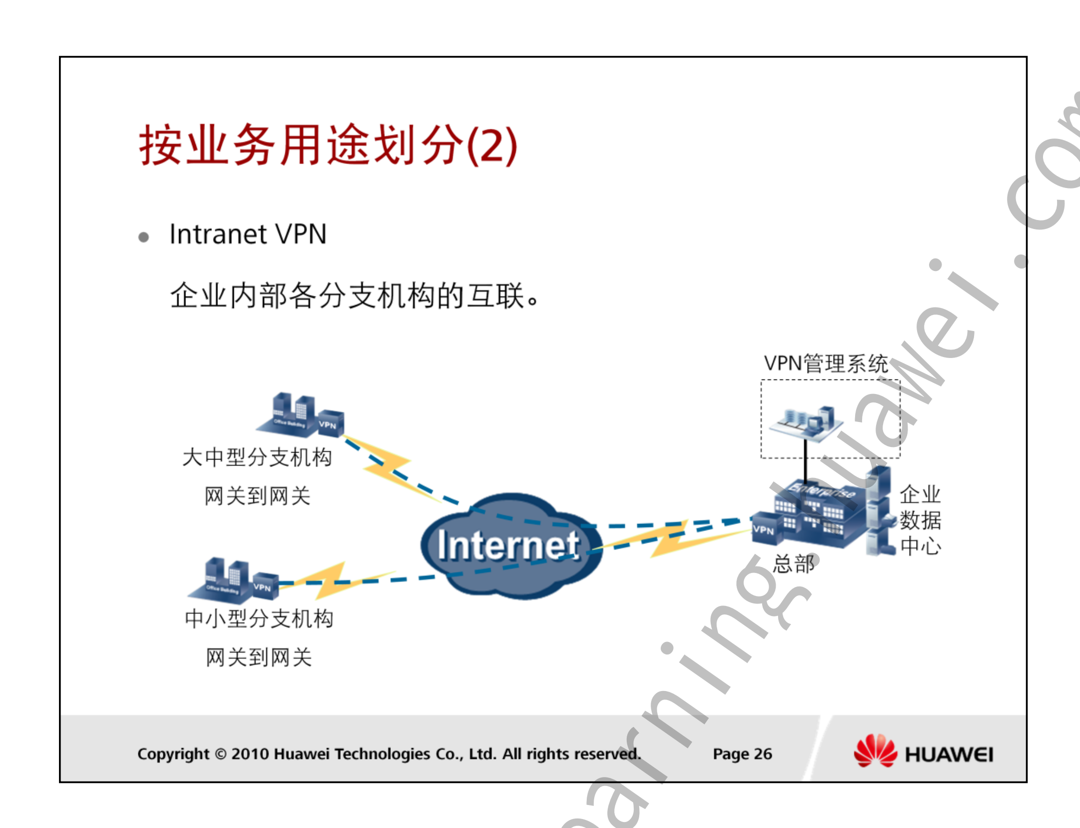
按照业务用途类型，可以将VPN划分为远程访问虚拟网（Access VPN）、企业内部虚拟网（Intranet VPN）和企业扩展虚拟网（Extranet VPN），这三种类型的VPN分别与传统的远程访问网络、企业内部的Intranet以及企业网和相关合作伙伴的企业网所构成的Extranet相对应。

- Access VPN

如果企业的内部人员移动或有远程办公需要，或者商家要提供B2C的安全访问服务，就可以考虑使用Access VPN。

Access VPN通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。AccessVPN能使用户随时、随地以其所需的方式访问企业资源。Access VPN包括模拟、拨号、ISDN、数字用户线路（xDSL）、移动IP和电缆技术，能够安全地连接移动用户、远程工作者或分支机构。

Access VPN最适用于公司内部经常有流动人员远程办公的情况。出差员工利用当地ISP提供的VPN服务，就可以和公司的VPN网关建立私有的隧道连接。



- Intranet VPN

如果要进行企业内部各分支机构的互联，使用Intranet VPN是很好的方式。

越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司、研究所等，各个分公司之间传统的网络连接方式一般是租用专线。显然，在分公司增多、业务开展越来越广泛时，网络结构趋于复杂，费用昂贵。利用VPN特性可以在Internet上组建世界范围内的Intranet VPN。利用Internet的线路保证网络的互联性，而利用隧道、加密等VPN特性可以保证信息在整个Intranet VPN上安全传输。Intranet VPN通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。企业拥有与专用网络的相同政策，包括安全、服务质量（QoS）、可管理性和可靠性。

按业务用途划分(3)

- Extranet VPN

  提供B2B（Business to Business）之间的安全访问服务。

VPN管理系统
客 户
Internet
企业数据中心
总部
供 应 商

 Page 27 HUAWEI

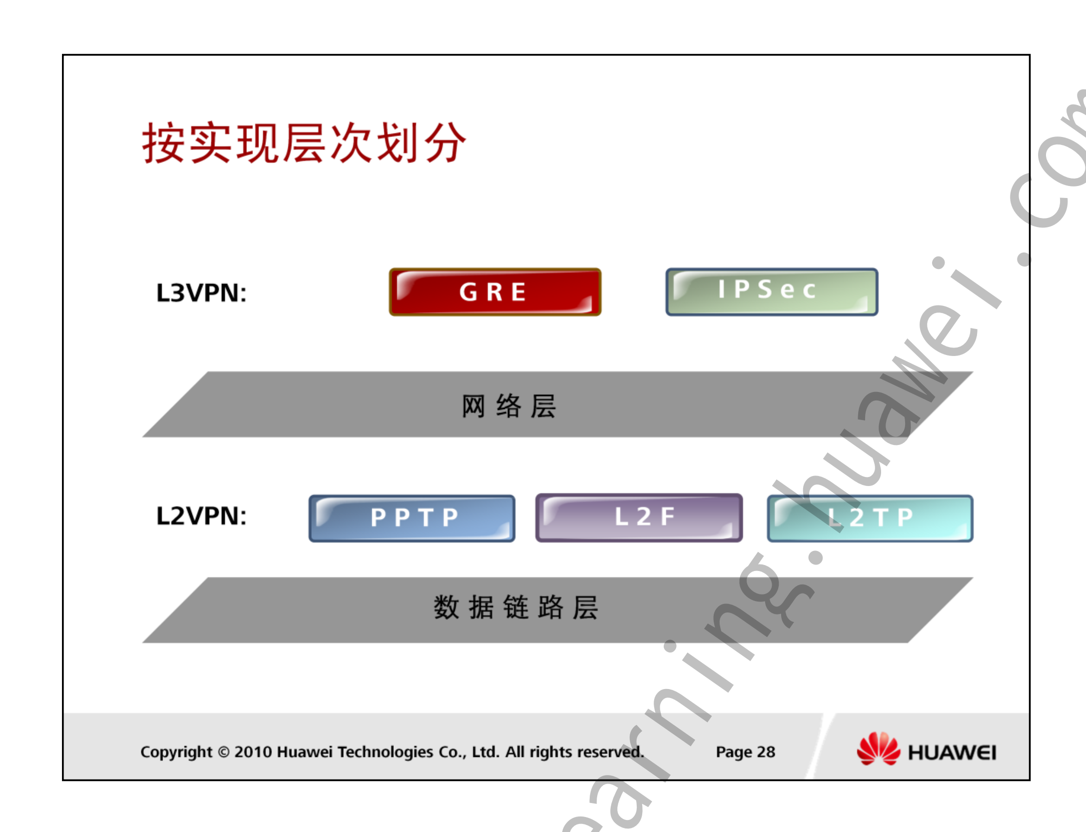
- Extranet VPN

如果是提供B2B（Business to Business）之间的安全访问服务，则可以考虑Extranet VPN。

随着信息时代的到来，各个企业越来越重视各种信息的处理。希望可以提供给客户最快捷方便的信息服务，通过各种方式了解客户的需要，同时各个企业之间的合作关系也越来越多，信息交换日益频繁。Internet为这样的一种发展趋势提供了良好的基础，而如何利用Internet进行有效的信息管理，是企业发展中不可避免的一个关键问题。利用VPN技术可以组建安全的Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络的安全。

Extranet VPN通过一个使用专用连接的共享基础设施，将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络的相同政策，包括安全、服务质量（QoS）、可管理性和可靠性。

Extranet VPN对用户的吸引力在于：能容易地对外部网进行部署和管理，外部网的连接可以使用与部署内部网和远端访问VPN相同的架构和协议进行部署。主要的不同是接入许可，外部网的用户只有在被许可时才有机会接入企业内网，访问特定的资源。



- L3VPN

三层VPN主要是指VPN技术工作在协议栈的网络层。以IPSec VPN技术为例，IPSec报头与IP报头工作在同一层次，封装报文时或者是以IPinIP的方式进行封装，或者是IPSec报头与IP报头同时对数据载荷进行封装。

除IPSec VPN技术外，主要的三层VPN技术还有GRE VPN。GRE VPN产生的时间比较早，实现的机制也比较简单。GRE VPN可以实现任意一种网络协议在另一种网络协议上的封装。与IPSec相比，安全性没有得到保证，只能提供有限的简单的安全机制。

- L2VPN

与三层VPN类似，二层VPN则是指VPN技术工作在协议栈的数据链路层，即数据链路层。二层VPN主要包括的协议有点到点隧道协议（PPTP, Point-to-Point Tunneling Protocol）、二层转发协议（L2F, Layer 2 Forwarding）以及二层隧道协议（L2TP, Layer 2 Tunneling Protocol）。



目录



VPDN概述

网络设备与VPDN网关

- 客户的PPP直接连接到企业的网关上，目前可使用的协议有L2F与L2TP

客户机与VPDN网关

- 客户机先建立与Internet的连接，再通过专用的客户软件（如Win2000支持的L2TP客户端）与网关建立通道连接。

- VPDN（Virtual Private Dial Network）是指利用公共网络（如ISDN和PSTN）的拨号功能及接入网来实现虚拟专用网，从而为企业、小型ISP、移动办公人员提供接入服务。
- VPDN隧道协议可分为PPTP、L2F和L2TP三种，目前使用最广泛的是L2TP

 Page 30



VPDN（Virtual Private Dial Network）是指利用公共网络（如ISDN 和PSTN）的拨号功能及接入网来实现虚拟专用网，从而为企业、小型ISP、移动办公人员提供接入服务。

VPDN采用专用的网络通信协议，在公共网络上为企业建立有一定安全性的虚拟专网。企业驻外机构和出差人员可从远程经由公共网络，通过虚拟隧道实现和企业总部之间的网络连接，而公共网络上其它用户则无法穿过虚拟隧道访问企业网内部的资源。

VPDN有下列两种实现方式:

1. 客户端通过NAS与VPDN网关建立隧道的方式。这种方式将客户的PPP连接直接连到企业的网关上，目前可使用的协议有L2F与L2TP等。其好处在于：对用户是透明的，用户只需要登录一次就可以接入企业网络，由企业网进行用户认证和地址分配，而不占用公共地址，用户可使用各种平台上网。这种方式需要NAS 支持VPDN 协议，需要认证系统支持VPDN 属性，网关一般使用防火墙或VPN 专用服务器。
2. 客户端与VPDN 网关直接建立隧道的方式。这种方式由客户机先建立与Internet的连接，再通过专用的客户软件（如Windows系统支持的L2TP客户端）与网关建立通道连接。其好处在于：用户上网的方式和地点没有限制，不需ISP介入。缺点是：用户需要安装专用的软件，受用户使用平台的限制，而且VPN维护难度较大。

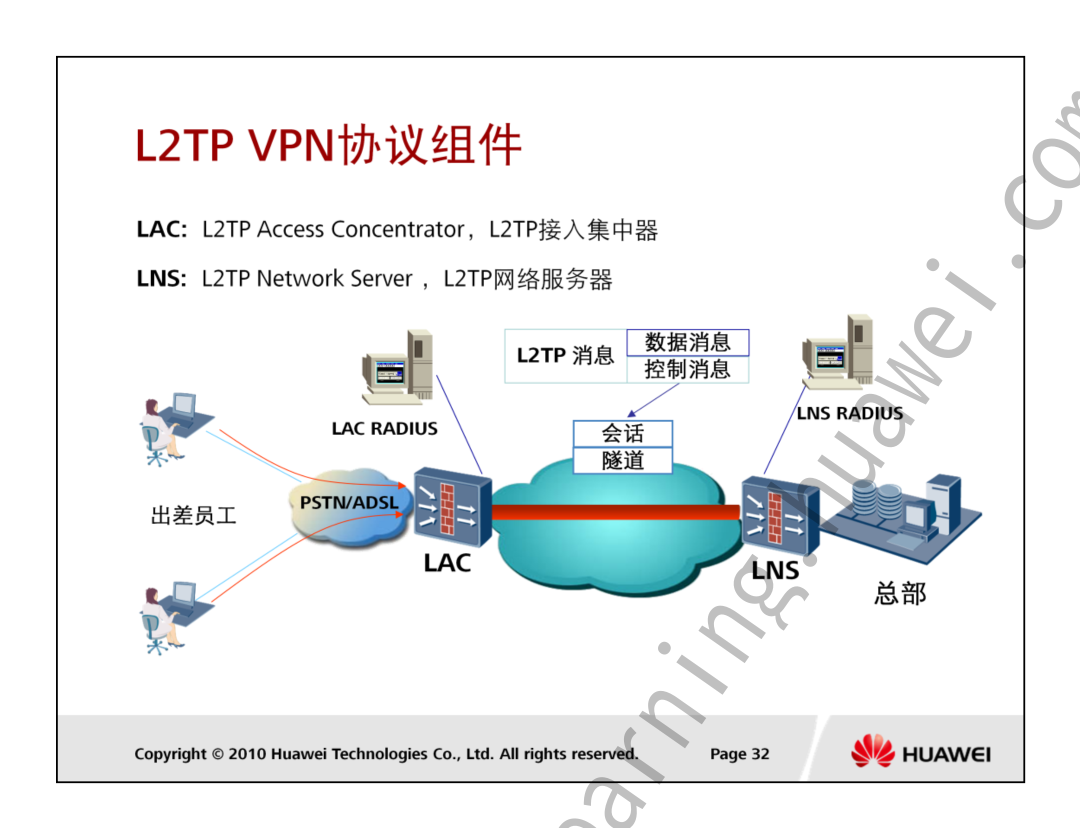
L2TP概述

- L2TP (Layer Two Tunneling Protocol) 二层隧道协议
  - 为在用户和企业的服务器之间透明传输PPP报文而设置的隧道协议。提供了对PPP 链路层数据包的通道（Tunnel）传输支持。
  - 结合了L2F 协议和PPTP 协议的各自优点，成为IETF 有关二层隧道协议的工业标准。
- 主要用途
  - 企业驻外机构和出差人员可从远程经由公共网络，通过虚拟隧道实现和企业总部之间的网络连接

 Page 31



L2TP（Layer 2 Tunnel Protocol）称为二层隧道协议，是为在用户和企业的服务器之间透明传输PPP报文而设置的隧道协议。PPP协议定义了一种封装技术，可以在二层的点到点链路上传输多种协议数据包，这时用户与NAS 之间运行PPP协议，二层链路端点与PPP会话点驻留在相同硬件设备上。L2TP协议提供了对PPP链路层数据包的通道（Tunnel）传输支持，允许二层链路端点和PPP会话点驻留在不同设备上并且采用包交换网络技术进行信息交互，从而扩展了PPP模型。从某个角度来讲，L2TP实际上是一种PPPoIP的应用，就像PPPoE、PPPoA、PPPoFR一样，都是一些网络应用想利用PPP的一些特性，弥补本网络自身的不足。另外，L2TP协议还结合了L2F协议和PPTP协议的各自优点，成为IETF有关二层隧道协议的工业标准。



在L2TP构建的VPDN中，协议组件包括以下三个部分：

- 远端系统

远端系统是要接入VPDN网络的远地用户和远地分支机构，通常是一个拨号用户的主机或私有网络的一台路由设备。

- LAC

LAC是附属在交换网络上的具有PPP端系统和L2TP协议处理能力的设备，通常是一个当地ISP的NAS，主要用于为PPP类型的用户提供接入服务。

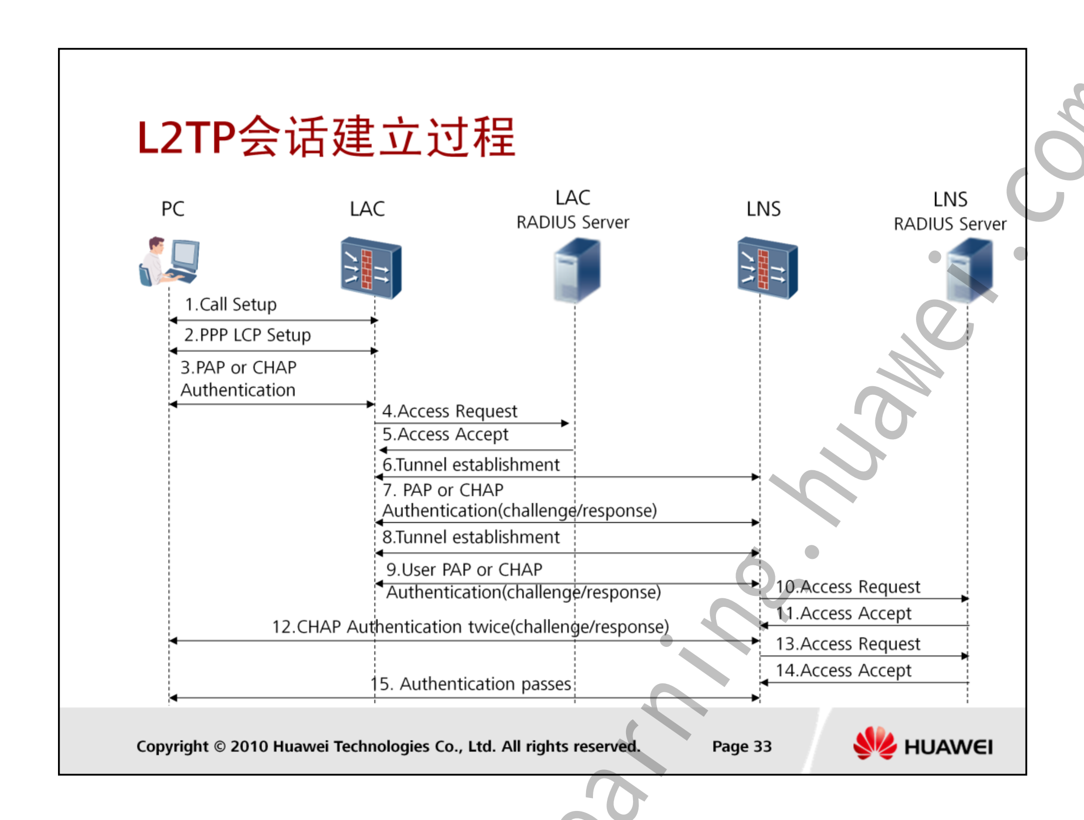
LAC位于LNS和远端系统之间，用于在LNS和远端系统之间传递信息包。它把从远端系统收到的信息包按照L2TP协议进行封装并送往LNS，同时也将从LNS收到的信息包进行解封装并送往远端系统。LAC与远端系统之间采用本地连接或PPP链路，VPDN应用中通常为PPP链路。

- LNS

LNS既是PPP端系统，又是L2TP协议的服务器端，通常作为一个企业内部网的边缘设备。

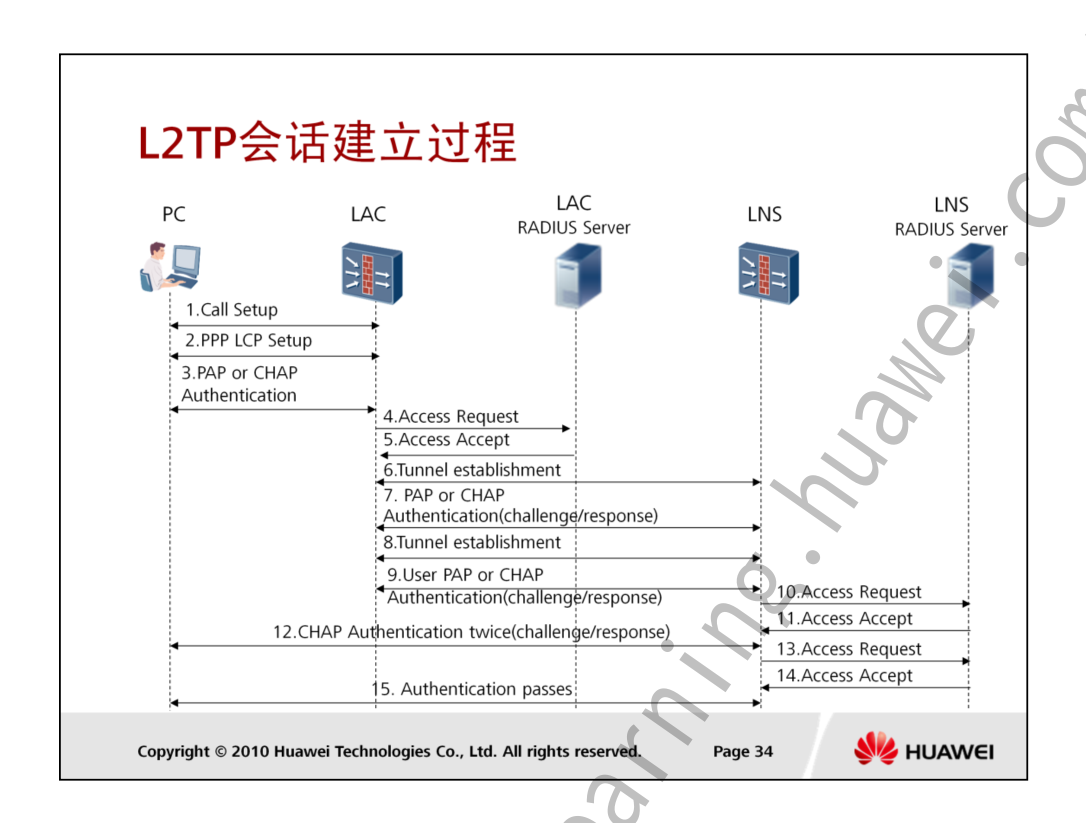
LNS作为L2TP隧道的另一侧端点，是LAC的对端设备，是LAC进行隧道传输的PPP会话的逻辑终止端点。通过在公网中建立L2TP隧道，将远端系统的PPP连接的另一端由原来的LAC在逻辑上延伸到了企业网内部的LNS。

L2TP中存在两种消息：控制消息和数据消息。控制消息用于隧道和会话连接的建立、维护及删除；数据消息则用于封装PPP帧并在隧道上传输。



L2TP会话建立过程:

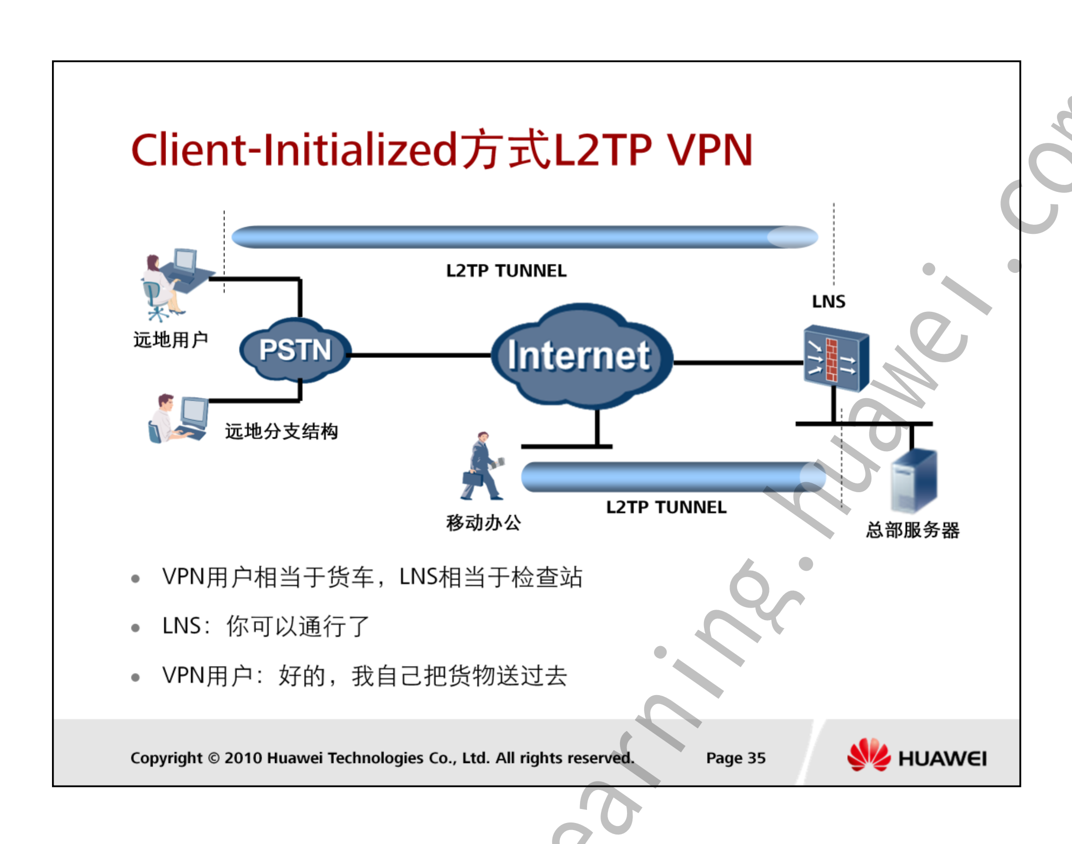
1. 用户端PC机发起呼叫连接请求。
2. PC机和LAC端进行PPP LCP协商。
3. LAC对PC机提供的用户信息进行PAP或CHAP认证。
4. LAC将认证信息（用户名、密码）发送给RADIUS服务器进行认证。
5. RADIUS服务器认证该用户，如果认证通过则返回该用户对应的LNS地址等相关信息，并且LAC准备发起Tunnel连接请求。
6. LAC端向指定LNS发起Tunnel连接请求。
7. LAC端向指定LNS发送CHAP challenge 信息，LNS回送该challenge响应消息CHAPresponse，并发送LNS 侧的CHAP challenge，LAC返回该challenge的响应消息CHAPresponse。需要注意：本阶段验证是对设备进行验证，不是对用户身份的认证。
8. 隧道验证通过，开始创建L2TP隧道。
9. 采用代理验证方式时，LAC端将用户CHAP response、response identifier和PPP协商参数传送给LNS。
10. LNS将接入请求信息发送给RADIUS服务器进行认证。
11. RADIUS服务器认证该请求信息，如果认证通过则返回响应信息。
12. 若用户在LNS侧配置强制本端CHAP认证，则LNS对用户进行认证，发送CHAP challenge，用户侧回应CHAP response。



13. LNS将接入请求信息发送给RADIUS服务器进行认证。

14. RADIUS服务器认证该请求信息，如果认证通过则返回响应信息。

15.验证通过，L2TP成功建立。



LAC表示L2TP访问集中器（L2TP Access Concentrator），是附属在交换网络上的具有PPP 端系统和L2TP协议处理能力的设备。LAC一般是一个网络接入服务器NAS，主要用于通过PSTN/ISDN 网络为用户提供接入服务。LNS表示L2TP网络服务器（L2TP Network Server），是PPP 端系统上用于处理L2TP协议服务器端部分的设备。

LAC客户端可直接向LNS发起隧道连接请求，无需再经过一个单独的LAC设备。LAC客户端地址的分配由LNS来完成。

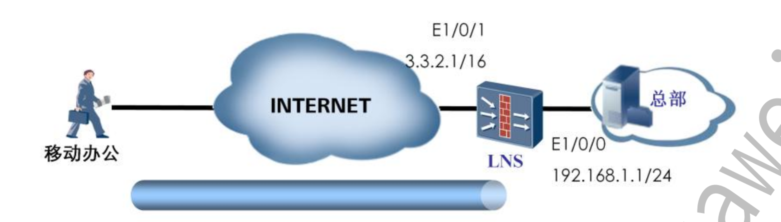
- 远程拨号用户发起

用户通过PSTN/ISDN接入ISP，获得访问Internet权限然后直接向远端LNS服务器发起L2TP连接。此时客户可直接向LNS发起通道连接请求，无需再经过一个单独的LAC设备。LAC客户地址的分配由LNS来完成。

这种方式的L2TP协议允许移动用户直接发起L2TP隧道连接，要求移动用户安装VPDN的客户端软件，需要知道LNS的IP地址。客户端软件可以是windows自带的L2TP VPN拨号软件，也可以是华为的secoway VPNClient。此类组网适用于移动用户上网访问企业网。

- 各组件的工作如下：
  - VPN Client: 首先获得公网地址，与LNS之间保持连通，向LNS发起建立隧道请求；
  - LNS: 为用户分配私网地址，准许用户接入内部网络。

Client-Initialized方式L2TP配置



- 组网需求
  - 某公司建有自己的VPN网络，在公司总部的公网出口处，放置了一台VPN网关，即USG防火墙。要求出差人员能够通过L2TP隧道与公司内部业务服务器进行通信。
  - LNS侧采用本地验证方式。其中：
    - LNS设备为USG防火墙

 Page 36



说明：若使用Windows自带L2TP客户端软件拨号请禁用IPSec功能项。

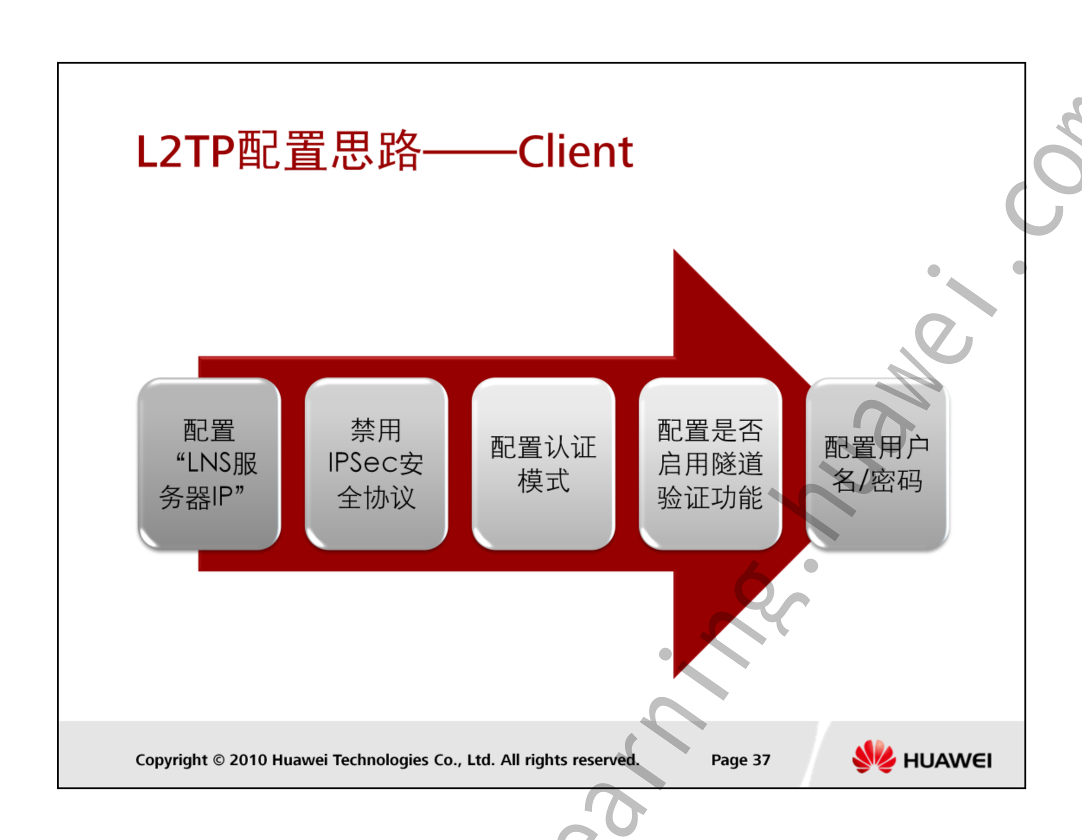
详细操作方法如下：

1、在“开始 > 运行”中，输入**regedit**命令，单击“确定”，进入注册表编辑器。

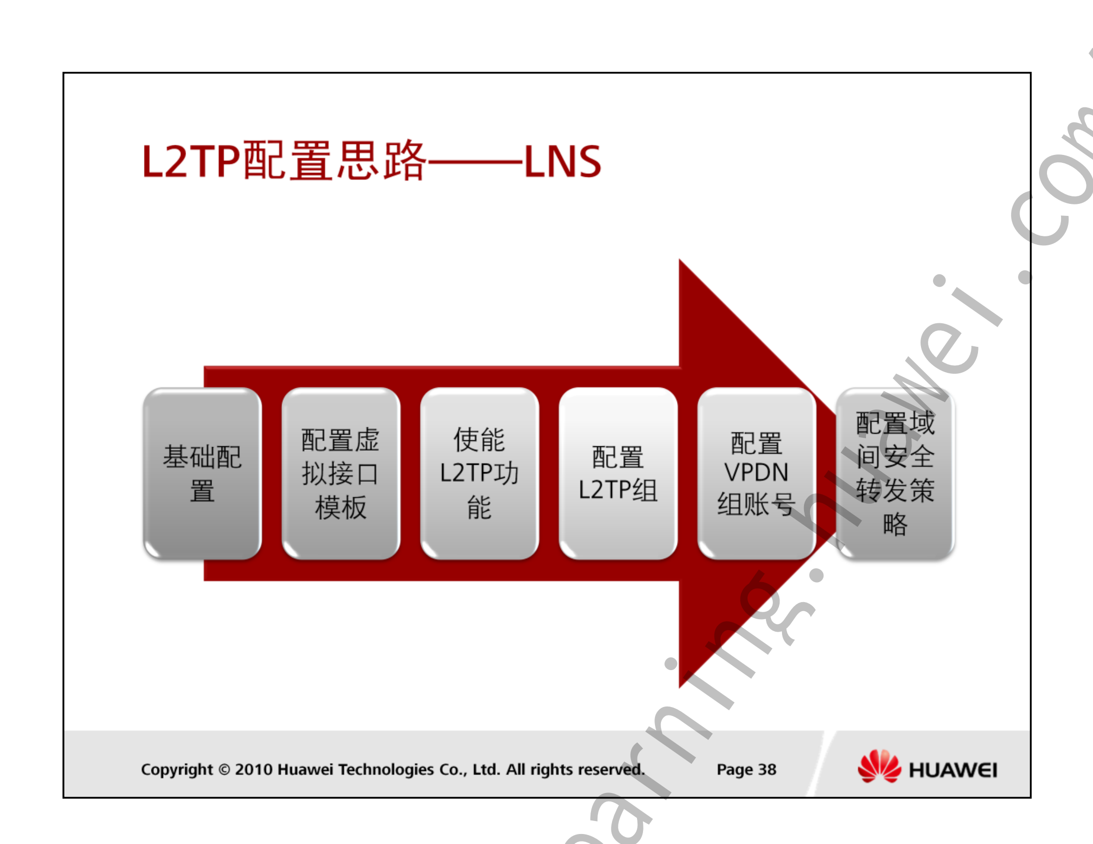
2、在界面左侧导航树中，定位至“我的电脑 > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > Rasman > Parameters”。在该路径下右侧界面中，检查是否存在名称为**ProhibitIpSec**、数据类型为DWORD的键值。如果不存在，请单击右键，选择“新建 > DWORD值”，并将名称命名为**ProhibitIpSec**。如果此键值已经存在，请执行下面的步骤。

3、选中该值，单击右键，选择“修改”，编辑DWORD值。在“数值数据”文本框中填写**1**，单击“确定”。

4、重新启动该PC，使修改生效。



Client侧设置设置的认证模式和隧道验证密码需要与LNS侧保持一致。


L2TP配置思路——LNS
基础配置
配置虚拟接口模板
使能L2TP功能
配置L2TP组
配置VPDN组账号
配置域间安全转发策略
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 38
HUAWEI

L2TP VPN典型配置—LNS(1)

- 创建虚拟接口模板。

  [LNS] interface Virtual-Template 1

  [LNS-Virtual-Template1] ip address 10.1.1.1 24

  [LNS-Virtual-Template1] ppp authentication-mode chap

  [LNS-Virtual-Template1] remote address pool 1

- 将虚拟接口模板加入安全区域。（步骤省略）
- 配置L2TP组。

  [LNS] l2tp enable

  [LNS] l2tp-group 1

  [LNS-l2tp1] allow l2tp virtual-template 1 （remote Client01）

  [LNS-l2tp1] tunnel authentication

  [LNS-l2tp1] tunnel password simple hello

  [LNS-l2tp1] tunnel name lns

 Page 39



- 配置虚拟接口模板加入安全区域的命令为：

  [LNS-zone-trust] add interface Virtual-Template 1

  说明：此处指定的地址池号需要与AAA视图下配置的地址池相对应。

  若增加“remote client01”命令，说明l2tp-group不是L2TP默认组，且将只接受指定的Client01隧道名客户端的呼叫，而不带“remote client01”命令，将说明L2TP-group 1为L2TP默认组，可接受任意的客户端呼叫。

  基于Client-Initialized方式L2TP若启动L2TP隧道认证，那么L2TP客户端软件需支持和启用才行，如华为Secospace vpn client客户端软件将带此功能。

  思考：L2TP默认组的主要作用？

L2TP VPN典型配置—LNS(3)

- 配置用户类型及账号密码。

  [LNS] aaa

  [LNS-aaa] local-user pc1 password simple pc1pc1

  [LNS-aaa] local-user pc1 service-type ppp

  [LNS-aaa] ip pool 1 4.1.1.1 4.1.1.99
- 配置域间缺省包过滤规则。

  [LNS] firewall packet-filter default permit interzone local untrust

 Page 40



- 进入AAA视图。

  [LNS] aaa

- 创建本地用户名和密码。

  [LNS-aaa] local-user pc1 password simple pc1pc1

- 配置用户类型。

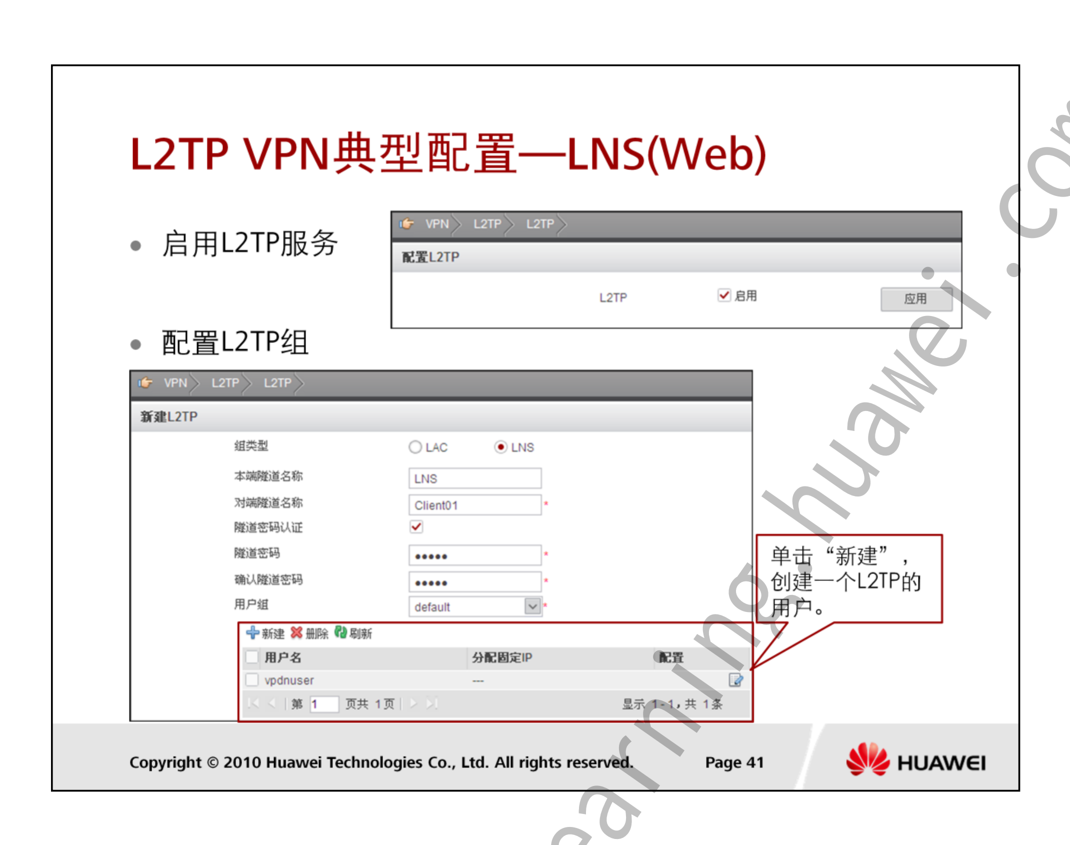
  [LNS-aaa] local-user pc1 service-type ppp

- 配置公共IP地址池。

  [LNS-aaa] ip pool 1 4.1.1.1 4.1.1.99

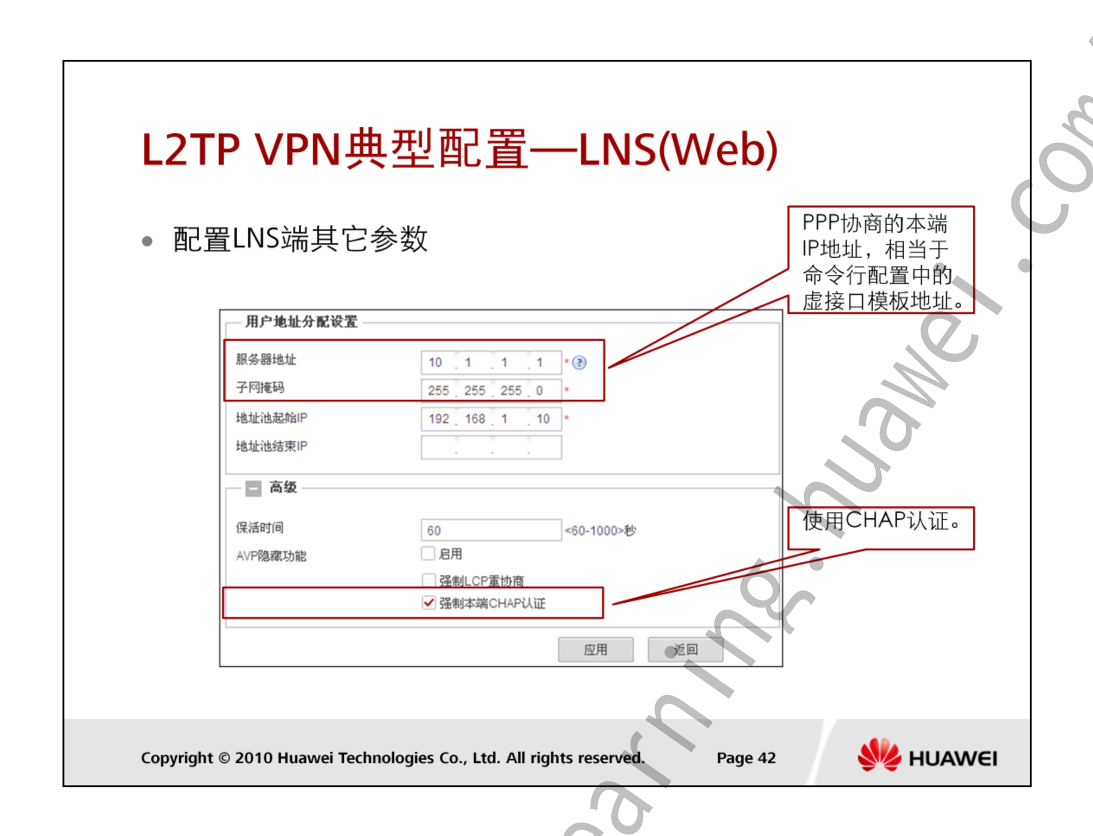
- 配置域间缺省包过滤规则。

  [LNS] firewall packet-filter default permit interzone local untrust



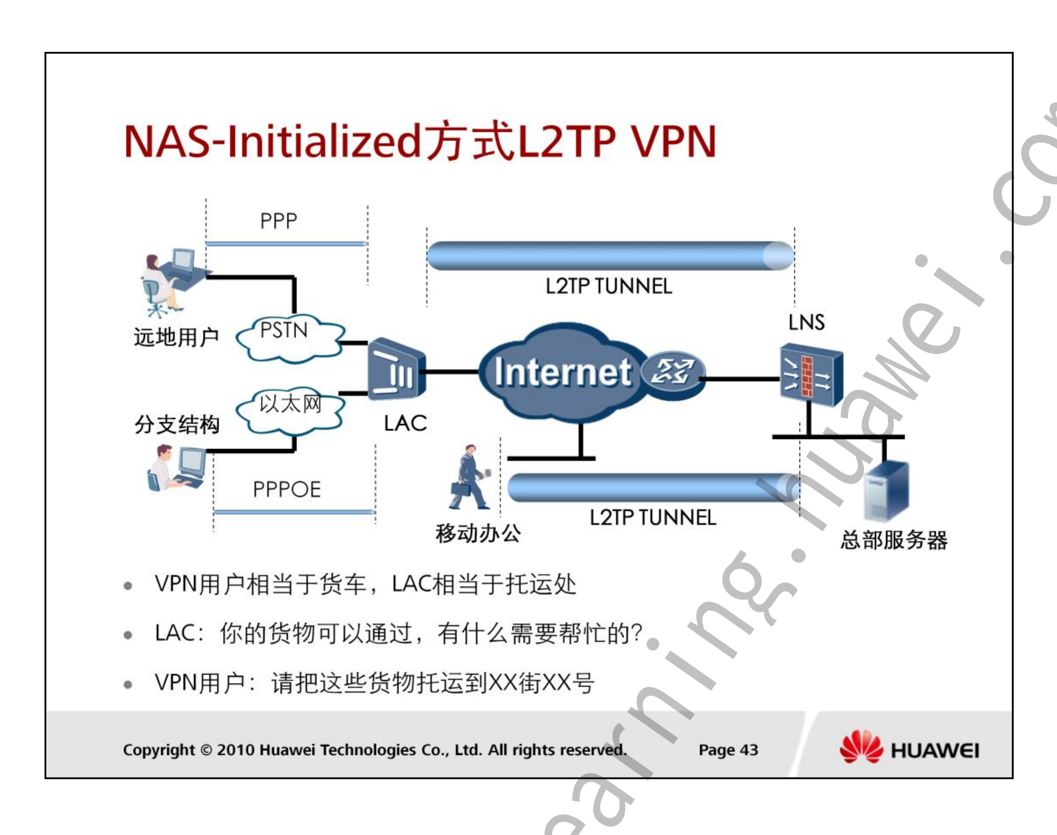
在Web配置界面下配置L2TP的步骤如下：

1. 选择“VPN > L2TP > L2TP”，
2. 在“配置L2TP”中，选中L2TP后的“启用”，单击“应用”。
3. 在“L2TP组列表”中，单击“新建”。
4. 选择“组类型”为“LNS”。
5. 依次输入其它参数。



服务器地址是PPP协商的本端IP地址。配置此IP地址后，才能保证PPP协商能够成功，从而保证拨号上线用户通过L2TP正常访问LNS端的内网服务器。

选中强制本端CHAP认证后表示在LAC对用户进行认证后，LNS对用户再次进行CHAP验证，如果验证不过，会话就不能建立成功。开启后可以提高安全性，但是会增加隧道建立时间。



用户通过PSTN/ISDN接入NAS(LAC)，LAC判断如果是VPN用户，由LAC通过Internet向LNS发起建立通道连接请求。拨号用户地址由LNS分配；对远程拨号用户的验证与计费既可由LAC侧的代理完成，也可在LNS侧完成。这种方式的L2TP协议，允许用户在接入到Internet的时候，通过BAS设备发起L2TP隧道连接。这个时候移动用户是不需要安装额外的VPDN软件的，但是必须采用PPP的方式接入到Internet，也可以是PPPOE等协议。

当在LAC设备上对用户的用户名、密码进行验证的时候，根据用户名就可以知道是L2TP隧道用户，然后自动向LNS设备发起连接，用户自然就接入到了自己的企业VPN中了。此方案适用于小型局域网访问公司总部网络。

- 各组件的工作如下：
  1. VPN Client: 向LAC设备发起PPP(或PPPOE)连接；
  2. LAC: 判断用户是否是L2TP用户，如果是，判断用户向哪个LNS发起隧道请求；
  3. LNS：为用户分配私网地址，准许用户接入内部网络。
- 对于这种方式的VPDN接入，主要有如下几个特点：
  1. 用户必须采用PPP的方式接入到Internet，比如PPPOE或者是传统的PPP拨号方式等
  2. 在运营商的接入设备上（主要是BAS设备）需要开通相应的VPN服务。
  3. 用户需要到运营商出申请这个业务。
  4. 对客户端没有任何要求，用户自己也感知不到已经接入到了企业网，完全是运营商来提供L2TP隧道服务。
  5. 一个隧道承载多个会话。

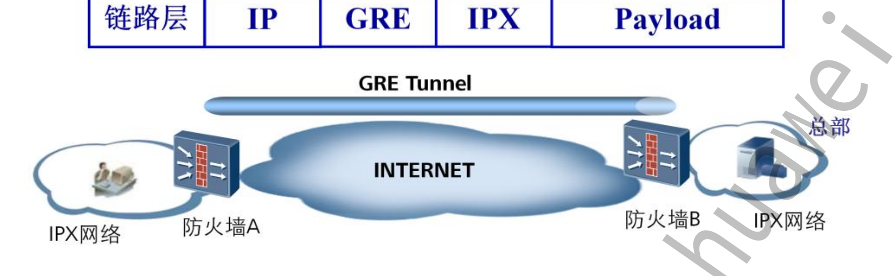


目录



GRE协议概述

链路层	IP	GRE	IPX	Payload



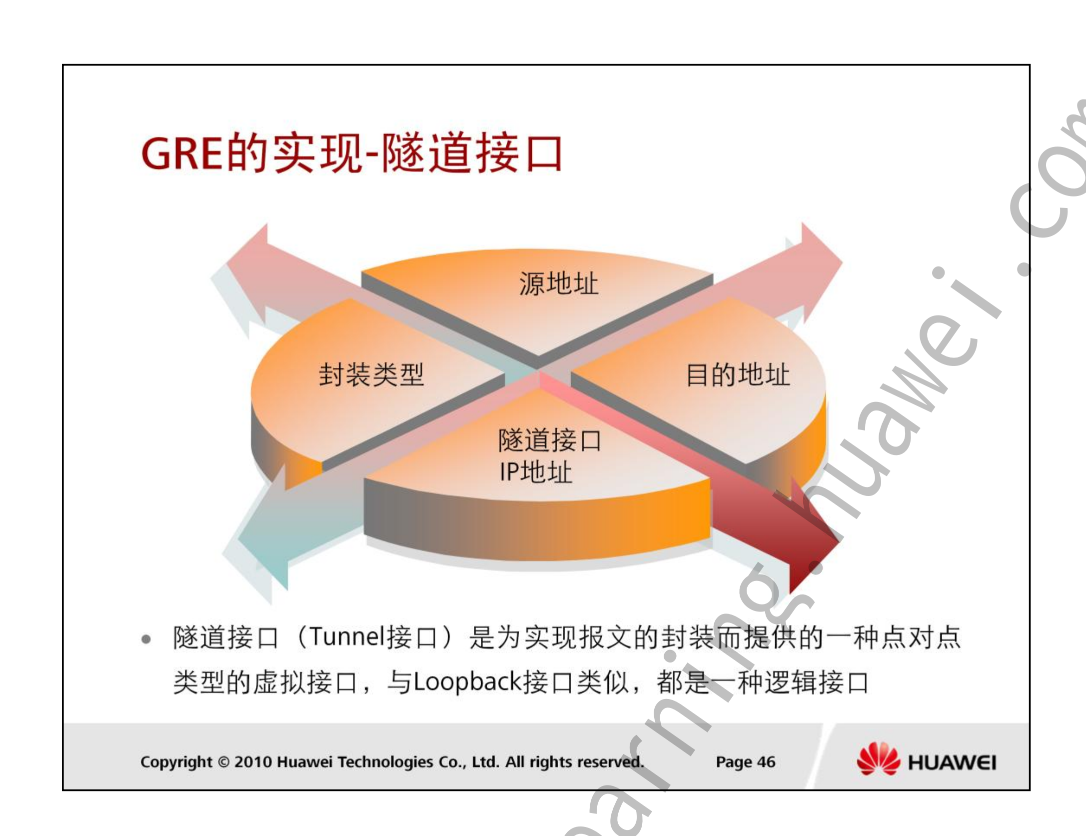
- GRE（Generic Routing Encapsulation）：是对某些网络层协议（如：IP，IPX，AppleTalk等）的数据报进行封装，使这些被封装的数据报能够在另一个网络层协议（如IP）中传输

 Page 45 

GRE（General Routing Encapsulation，通用路由封装）是对某些网络层协议（如IPX）的报文进行封装，使这些被封装的报文能够在另一网络层协议（如IP）中传输。

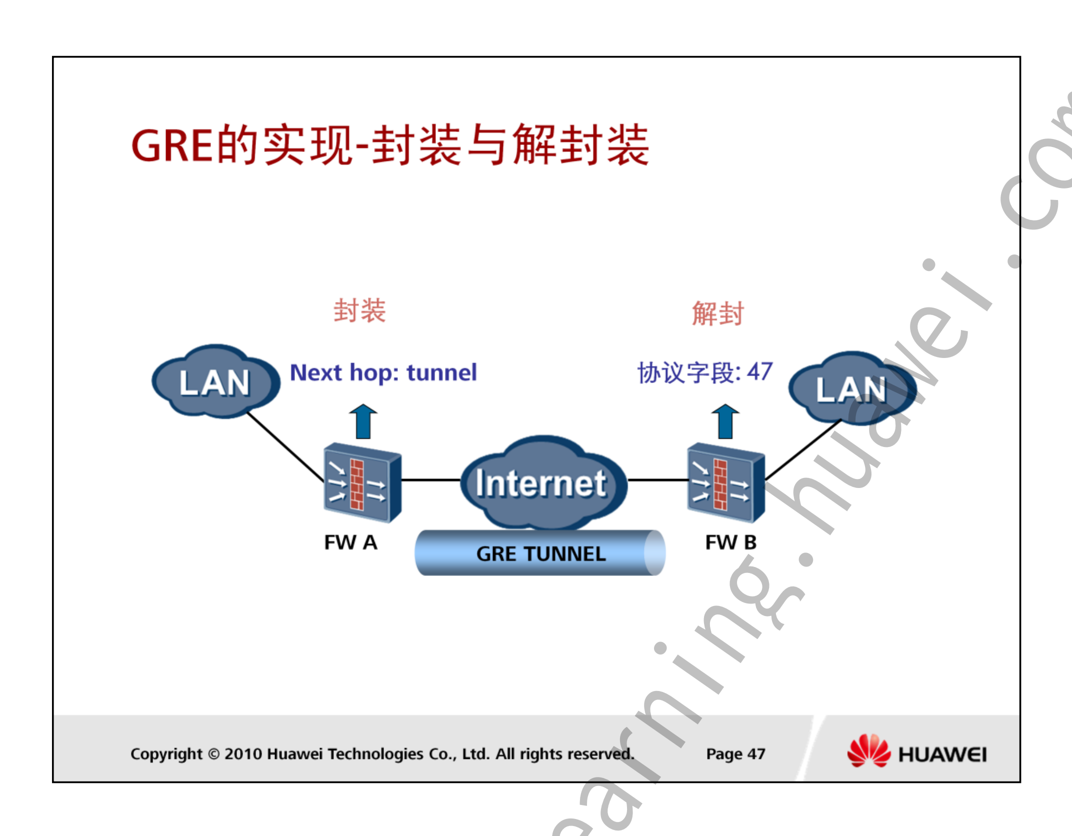
GRE提供了将一种协议的报文封装在另一种协议报文中的机制，使报文能够在异种网路中传输，封装后报文的传输通道称为tunnel。

Tunnel是一个虚拟的点对点的连接，可以看成仅支持点对点连接的虚拟接口，这个接口提供了一条通路，使封装的数据报能够在这个通路上传输，并在一个Tunnel的两端分别对数据报进行封装及解封装。



- 隧道接口包含以下元素：
  - 源地址：报文传输协议中的源地址。从负责封装后报文传输的网络来看，隧道的源地址就是实际发送报文的接口IP地址。
  - 目的地址：报文传输协议中的目的地址。从负责封装后报文传输的网络来看，隧道本端的目的地址就是隧道目的端的源地址。
  - 隧道接口IP地址：为了在隧道接口上启用动态路由协议，或使用静态路由协议发布隧道接口，要为隧道接口分配IP地址。隧道接口的IP地址可以不是公网地址，甚至可以借用其他接口的IP地址以节约IP地址。但是当Tunnel接口借用IP地址时，由于Tunnel接口本身没有IP地址，无法在此接口上启用动态路由协议，必须配置静态路由或策略路由才能实现路由器间的连通性。
  - 封装类型：隧道接口的封装类型是指该隧道接口对报文进行的封装方式。一般情况下有四种封装方式，分别是GRE、MPLS TE、IPv6-IPv4 和IPv4-IPv6。

经过手工配置，成功建立隧道之后，就可以将隧道接口看成是一个物理接口，可以在其上运行动态路由协议或配置静态路由。



报文在GRE 隧道中传输包括封装和解封装两个过程。以图的网络为例，如果私网报文从防火墙A（FW A）向防火墙B（FW B）传输，则封装在FW A上完成；而解封装在FW B上进行。

FW A 从连接私网的接口接收到私网报文后，首先交由私网上运行的协议模块处理。

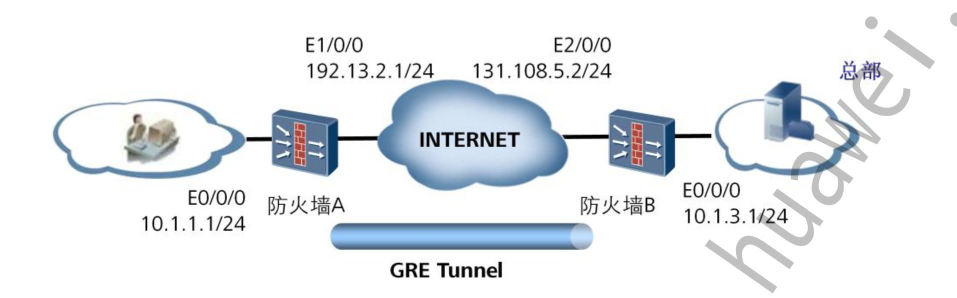
私网协议模块检查私网报文头中的目的地址并在私网路由表或转发表中查找出接口，确定如何路由此包。如果发现出接口是Tunnel接口，则将此报文发给隧道模块。

隧道模块收到此报文后进行如下处理：

1. 隧道模块根据乘客报文的协议类型和当前GRE隧道所配置的Key和Checksum参数，对报文进行GRE 封装，即添加GRE头。
2. 根据配置信息（传输协议为IP），给报文加上IP头。该IP头的源地址就是隧道源地址，IP头的目的地址就是隧道目的地址。
3. 将该报文交给IP模块处理，IP模块根据该IP头目的地址，在公网路由表中查找相应的出接口并发送报文。之后，封装后的报文将在该IP公共网络中传输。

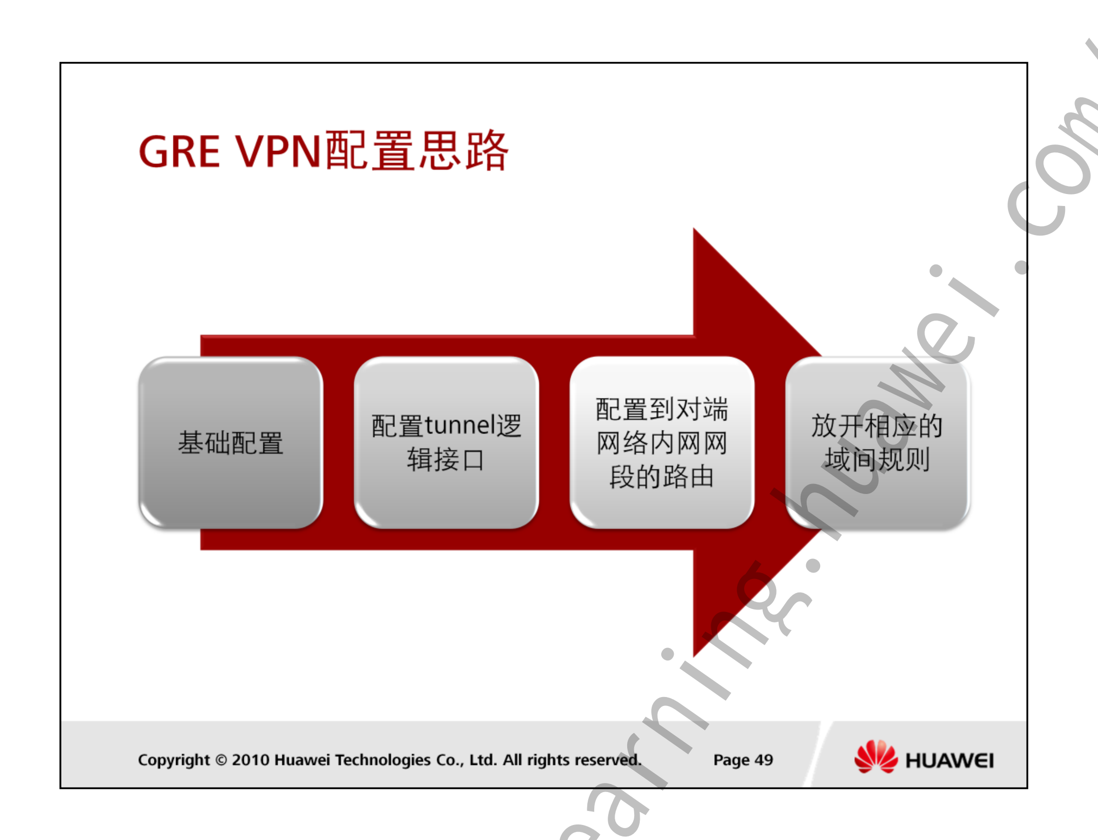
解封装过程和封装过程相反。FW B从连接公网的接口收到该报文，分析IP 头发现报文的目的地址为本设备，且协议字段值为47，表示协议为GRE（参见RFC1700），于是交给GRE 模块处理。GRE 模块去掉IP头和GRE 报头，并根据GRE头的Protocol Type字段，发现此报文的乘客协议为私网上运行的协议，于是交由此协议处理。此协议像对待一般数据报一样对此数据报进行转发。

GRE VPN典型应用场景描述



- 运行IP协议的两个子网网络1和网络2，通过在防火墙A和防火墙 B之间使用三层隧道协议GRE实现互联。





配置tunnel逻辑接口时，需要指定GRE隧道使用的源地址及目的地址。配置到对端网络内网网段的路由时，下一跳为tunnel口。

GRE VPN典型配置(命令行)

- 配置防火墙 A。
  - 基本配置（略）。
  - 创建并配置Tunnel1接口

```
[USG_A] interface tunnel 1
[USG_A-Tunnel1] ip address 10.1.1.1 24
[USG_A-Tunnel1] tunnel-protocol gre
[USG_A-Tunnel1] source 192.13.2.1
[USG_A-Tunnel1] destination 131.108.5.2
```

  - 配置从防火墙 A经过Tunnel1接口到Group2的静态路由。

```
[USG_A] ip route-static 10.1.3.0 255.255.255.0 tunnel 1
```

  - 将tunnel 1 加入Untrust区域，并配置相应域间转发策略。(略)
- 防火墙B的配置与A基本一致，只需调换隧道的源地址和目的地址以及默认路由。（略）



GRE VPN有如下一些关键配置：

- 创建虚拟Tunnel接口
- 配置Tunnel接口的源端地址
- 配置Tunnel接口的目的端地址。（Tunnel的源端地址与目的端地址唯一标识了一个通道，两端地址应互为源地址和目的地址。）
- 配置Tunnel接口的网络地址
- 防火墙域间转发策略

防火墙B的配置与A基本一致，命令行参考配置如下：

```
[B-Tunnel1] ip address 10.1.3.1 24
[B-Tunnel1] source 131.108.5.2
[B-Tunnel1] destination 192.13.2.1
```

配置从防火墙 B经过Tunnel1接口到Group1的静态路由。

```
[B] ip route-static 10.1.1.0 255.255.255.0 tunnel 1
```

GRE VPN典型配置(命令行)

- 配置防火墙 A。
  - 基本配置（略）。
  - 创建并配置Tunnel1接口

    [USG_A] interface tunnel 1

    [USG_A-Tunnel1] ip address 10.1.1.1 24

    [USG_A-Tunnel1] tunnel-protocol gre

    [USG_A-Tunnel1] source 192.13.2.1

    [USG_A-Tunnel1] destination 131.108.5.2
  - 配置从防火墙 A经过Tunnel1接口到Group2的静态路由。

    [USG_A] ip route-static 10.1.3.0 255.255.255.0 tunnel 1
  - 将tunnel 1 加入Untrust区域，并配置相应域间转发策略。(略)
- 防火墙B的配置与A基本一致，只需调换隧道的源地址和目的地址以及默认路由。（略）



GRE VPN典型配置(Web)

VPN > GRE > GRE

新建GRE接口

接口名称 Tunnle1 *
安全区域 untrust *
IP地址 10.1.1.1
掩码 255.255.255.0
隧道源IP配置方式 IP地址 接口
源IP地址 192.13.2.1
隧道目的IP配置方式 IP地址 域名
目的IP地址 131.108.5.2
隧道校验 启用
隧道识别关键字 <0-4294967295>
应用 返回

配置Tunnel接口的源地址和目的地址。

隧道验证和关键字识别作为GRE VPN的安全机制，为可选配置。

 Page 52 HUAWEI

在Web配置界面中，配置GRE VPN的操作步骤如下：

1. 选择“VPN > GRE > GRE”。
2. 在“GRE接口列表”中，单击“新建”。
3. 依次输入或选择GRE接口各项参数。
4. 单击“应用”。

隧道校验开启后，GRE隧道两端会进行端到端校验和的验证。

配置隧道识别关键字后，隧道双方将进行通道识别关键字的验证。只有隧道两端设置的识别关键字完全一致时才能通过验证，否则将报文丢弃。

IPSec VPN简介

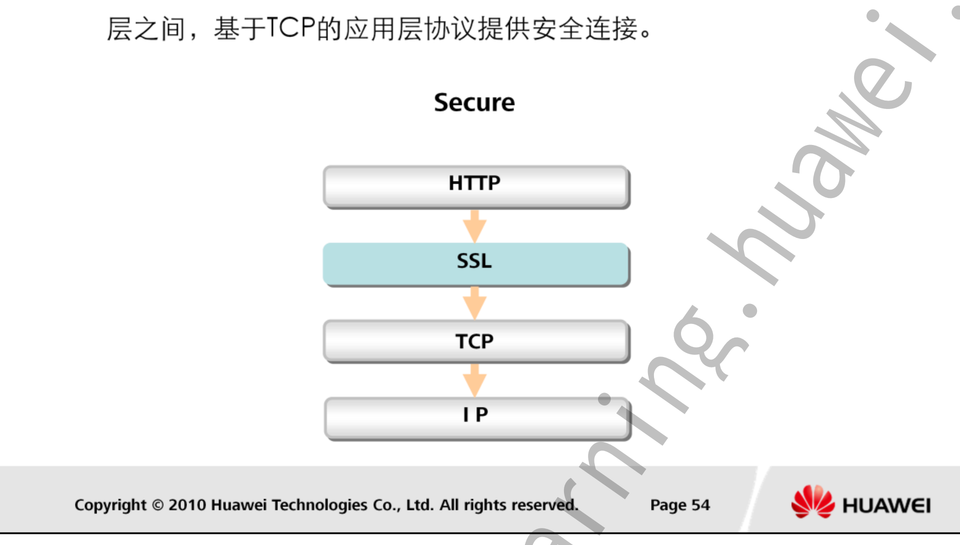
- IPSec（Internet Protocol Security）是一个工业标准网络安全协议，为IP网络通信提供透明的安全服务，保护TCP/IP通信免遭窃听和篡改，可以有效抵御网络攻击，同时保持易用性。属于三层VPN。
- IPSec的三个协议：

AH协议	ESP协议
IKE密钥交换协议	

 Page 53 

IPSec协议是特定的通信方之间在IP层通过加密与数据源验证等方式，来保证数据报在网络上传输时的私有性、完整性、真实性和防重放。

IPSec VPN将在后面章节详细介绍。



SSL是一种安全协议，可以分为SSL记录协议（SSL record protocol）、SSL握手协议（SSL handshake protocol）、SSL密码变化协议（SSL change cipher spec protocol）和SSL警告协议（SSL alert protocol）。

SSL VPN将在后面章节详细介绍。



总结

- VPN概念
- VPN关键技术
- VPN分类及应用



思考题

- 对称加密与非对称加密各有什么特点?
- 加密算法与散列算法有什么不同?
- 密钥长度长一定加密强度强吗?
- 隧道技术在VPN技术中有哪些主要作用?
- 为什么说L2TP是二层VPN，而GRE和IPSEC是三层VPN?
- L2TP VPN主要可以提供哪些安全服务？有哪些局限性?
- GRE VPN主要应用在哪些场景？它有什么局限性?



Thank you

www.huawei.com

HC110310009

HCNA-Security-CBSN 第九章 IPSec VPN 技术

第九章

IPSec VPN技术

www.huawei.com

HUAWEI



目标

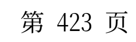
- 学完本课程后，您将能够:
  - 理解IPSec技术的基本原理
  - 理解AH和ESP技术
  - 了解IKE协议的业务流程
  - 掌握IPSec VPN的应用场景及配置





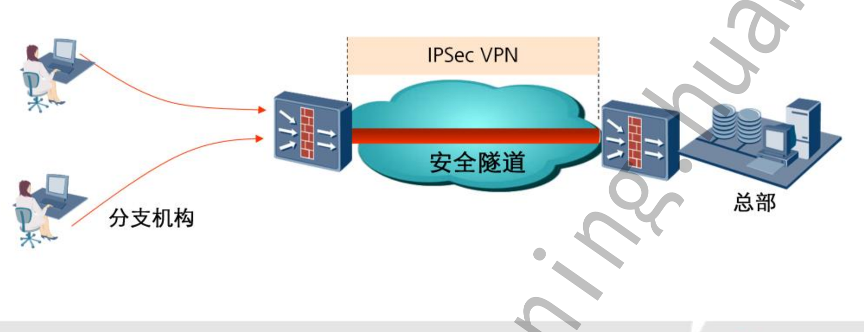
目录





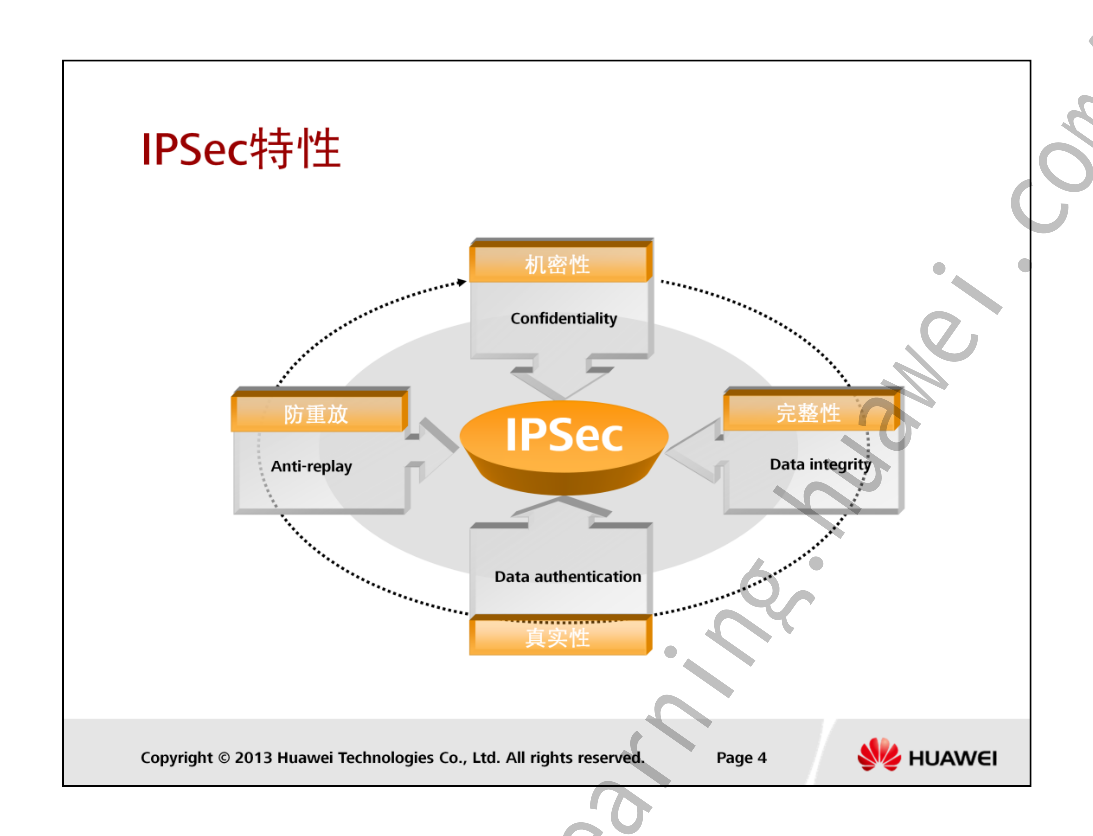
IPSec简介

- IPSec（IP Security）协议族是IETF制定的一系列安全协议，它为端到端IP报文交互提供了基于密码学的、可互操作的、高质量的安全保护机制。IPSec VPN是利用IPSec隧道建立的网络层VPN。

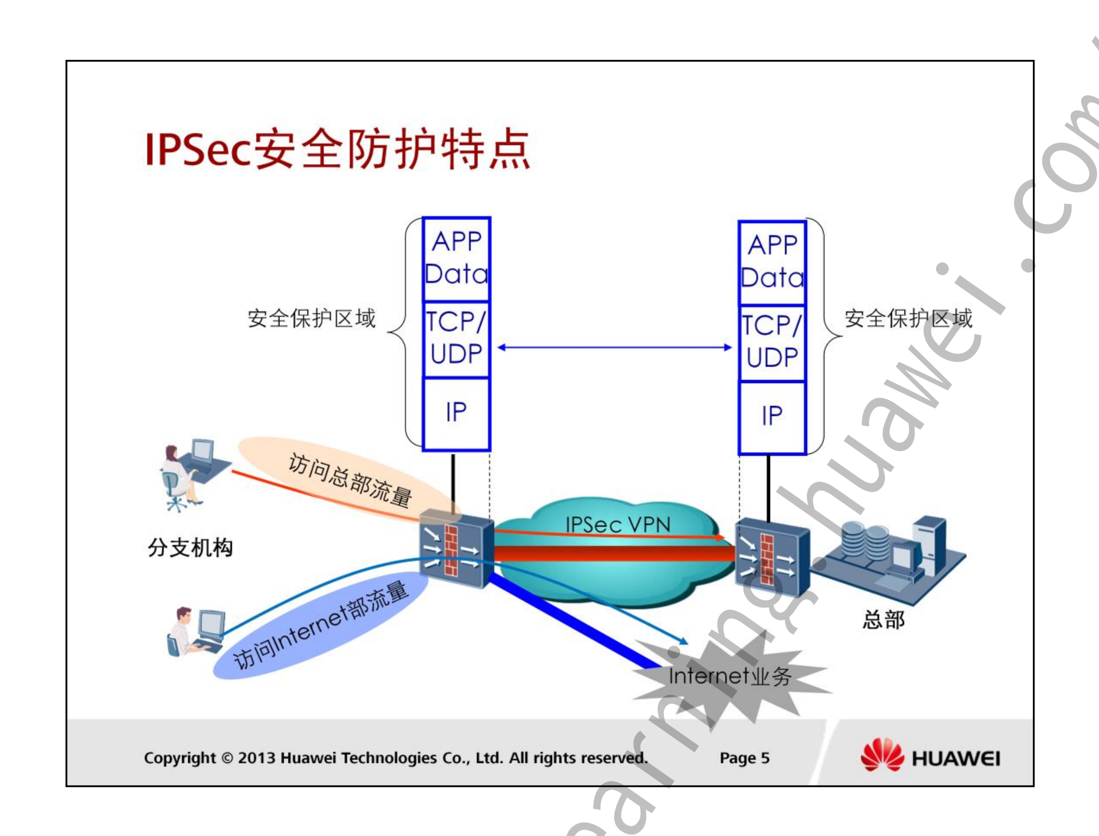




HUAWEI



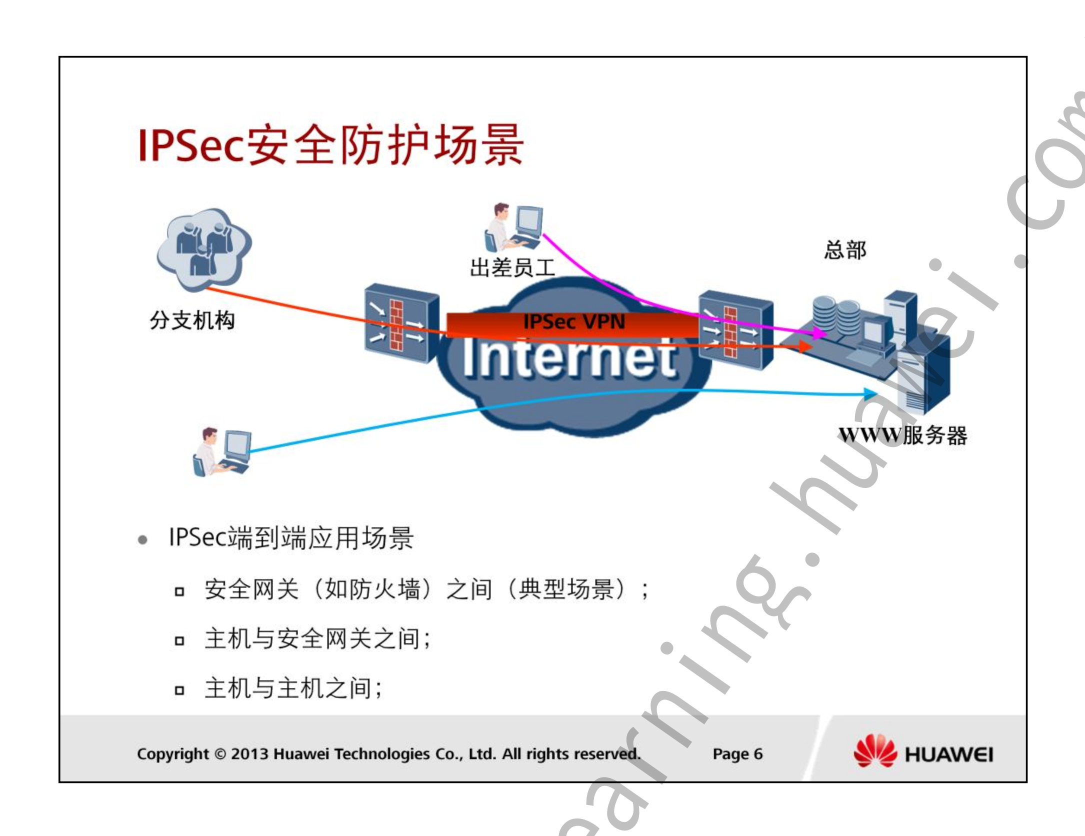
- 机密性：对数据进行加密，确保数据在传输过程中不被其它人员查看；
- 完整性：对接收到数据包进行完整性验证，以确保数据在传输过程中没有被篡改；
- 真实性：验证数据源，以保证数据来自真实的发送者（IP报文头内的源地址）；
- 抗重放：防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。



支持在IP层及以上协议层进行数据安全保护，并对上层应用透明（无需对各个应用程序进行修改）。安全保护措施包括机密性、完整性、真实性和抗重放等。

IPSec协议基于策略对数据包进行安全保护，如对某业务数据流采用某类保护措施，而对另一类业务数据流采用其它类保护措施，或不进行任何保护措施。

本图例中，访问总部的流量实施安全保护，而对于访问互联的流量，则不进行安全保护。



当分布于不同地域的企业或个人通过Internet进行通信时，由于处于不同的物理地域，它们之间进行通信的绝大部分流量都需要穿越Internet上的未知网络，无法保证在网络上发送和接收数据的安全性。

IPSec提供了一种建立和管理安全隧道的方式，通过对要传输的数据报文提供认证和加密服务来防止数据在网络内或通过公网传输时被非法查看或篡改，相当于为位于不同地域的用户创建了一条安全的通信隧道。

应用场景主要由以下三种类型：

- 网关（如防火墙）之间

此种应用场景也叫点到点或点到多点IPSec VPN，主要用于公司总部与分支机构之间建立IPSec隧道，从而实现局域网之间互通。

- 主机与网关之间

主要用于出差员工通过互联网需要访问总部资源时。

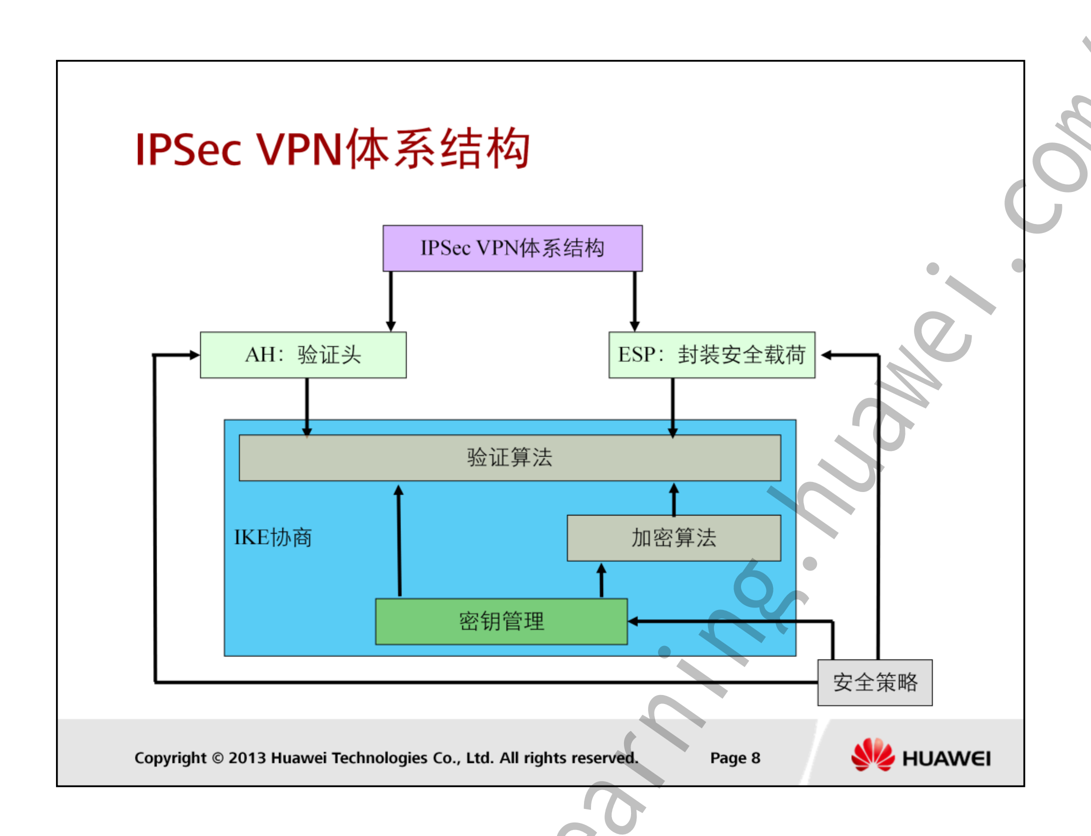
- 主机与主机之间

主机之间通过互联网进行数据传输，需要加密时，加解密操作在主机侧完成。某些场景中，例如服务器放在DMZ区域，防火墙配置NAT server,也可以实现。



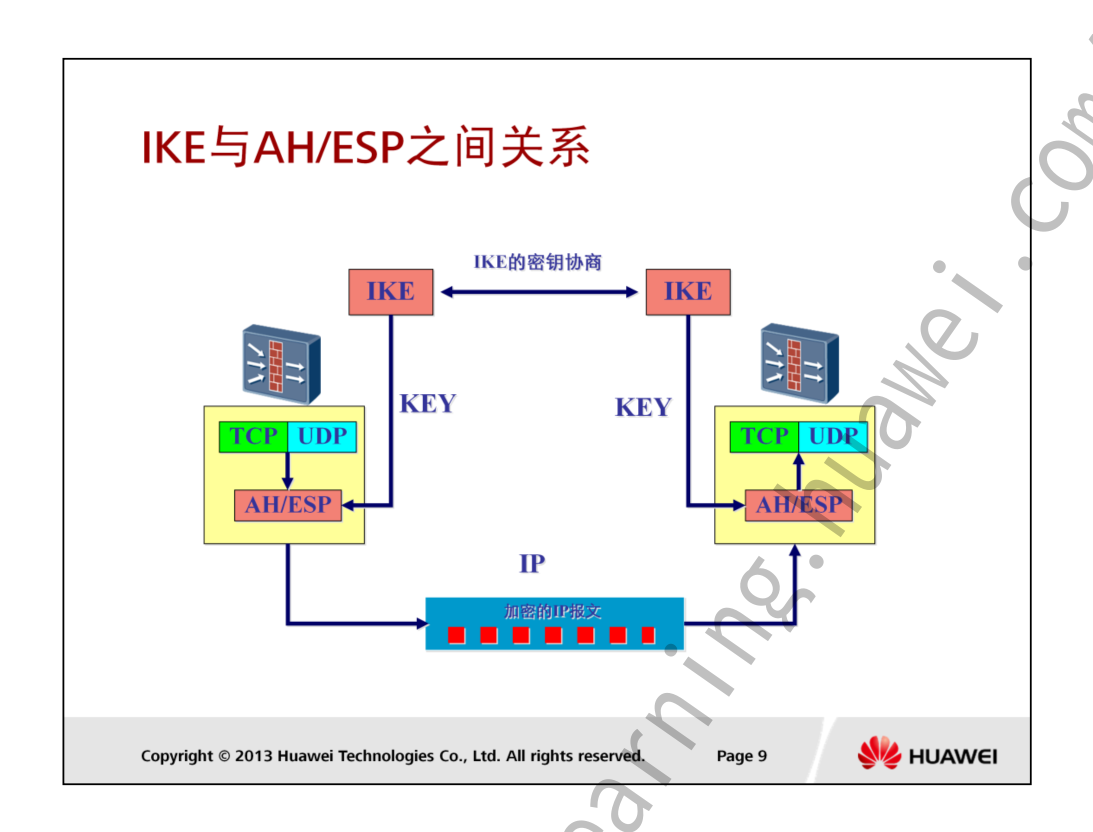
目录





IPSec VPN体系结构主要由AH、ESP和IKE协议套件组成。IPSec通过ESP来保障IP数据传输过程的机密性，使用AH/ESP提供数据完整性、数据源验证和抗报文重放功能。ESP和AH定义了协议和载荷头的格式及所提供的服务，但却没有定义实现以上能力所需具体转码方式，转码方式包括对数据转换方式，如算法、密钥长度等。为简化IPSec的使用和管理，IPSec还可以通过IKE进行自动协商交换密钥、建立和维护安全联盟的服务。具体介绍如下：

- AH协议：AH是报文头验证协议，主要提供的功能有数据源验证、数据完整性校验和防报文重放功能。然而，AH并不加密所保护的数据报。
- ESP协议：ESP是封装安全载荷协议。它除提供AH协议的所有功能外（但其数据完整性校验不包括IP头），还可提供对IP报文的加密功能。
- IKE协议：IKE协议用于自动协商AH和ESP所使用的密码算法。



IKE是UDP之上的一个应用层协议，是IPSec的信令协议。IKE为IPSec协商生成密钥,供AH/ESP加解密和验证使用。AH协议和ESP协议有自己的协议号，分别是51和50。

IPSec安全协议



- AH（Authentication Header）报文头验证协议，主要提供的功能有数据源验证、数据完整性校验和防报文重放功能；然而，AH并不加密所保护的数据报文。

ESP

- ESP（Encapsulating Security Payload）ESP是封装安全载荷协议。它除提供AH协议的所有功能外（但其数据完整性校验不包括IP头），还可提供对IP报文的加密功能。

- IPSec通过AH（Authentication Header）和ESP（Encapsulating Security Payload）这两个安全协议来实现数据报文在网络上传输时的私有性、完整性、真实性和防重放。

 Page 10



AH和ESP是IPSec的两个主要协议。认证头（AH，Authentication Header）协议为IP通信提供数据源认证、数据完整性检验和防重放保证。封装安全载荷（ESP，Encapsulating Security Payload）为IP通信提供完整性检验、认证、加密和防重放保证。

AH和ESP可以单独使用，也可以同时使用。 在实际的组网中,ESP协议使用较多。

IPSec协议封装模式

传输模式
- 在传输模式下，IPSec头被插入到IP头之后但在所有传输层协议之前，或所有其他IPSec协议之前。

隧道模式
- 在隧道模式下， IPSec头插在原始IP头之前，另外生成一个新的报文头放到AH或ESP之前。

传输模式

IPH Data

IPH IPSec Data

隧道模式

New IPH IPSec Org IPH Data

 Page 11 HUAWEI

IPSec协议有两种封装模式：传输模式和隧道模式。

在传输模式下，IPSec协议处理模块会在IP报头和高层协议报头之间插入一个IPSec报头。在这种模式下，IP报头与原始IP分组中的IP报头是一致的，只是IP报文中的协议字段会被改成IPSec协议的协议号（50或者51），并重新计算IP报头校验和。传输模式保护数据包的有效载荷、高层协议，IPSec源端点不会修改IP报头中目的IP地址，原来的IP地址也会保持明文。传输模式只为高层协议提供安全服务。这种模式常应用在需要保护的两台主机之间的端到端连接，而不是多台主机的两个网关之间的数据流。

与传输模式不同，在隧道模式下，原始IP分组被封装成一个新的IP报文，在内部报头以及外部报头之间插入一个IPSec报头，原IP地址被当作有效载荷的一部分收到IPSec的保护。另外，通过对数据加密，还可以隐藏原数据包中的IP地址，这样更有利于保护端到端通信中数据的安全性。

- 传输模式（Transport Mode）：

  1）应用场景1：主机与网络安全网关之间的通信；

  2）应用场景2：主机与主机之间的通信。

- 隧道模式（Tunnel Mode）：

  1）应用场景：网络安全网关与网络安全网关之间的通信。

IPSec协议封装模式对比

传输模式：

原IP头	IPSec头	IP数据

隧道模式：

新IP头	IPSec头	原IP头	原IP数据

- 封装模式对比：
  - 安全性：
    - 隧道模式隐藏原IP头信息，安全性更好。
  - 性能：
    - 隧道模式有一个额外的IP头，隧道模式比传输模式占用更多带宽。
  - 具体选择那封装模式，需要在性能和安全之间做权衡。

加密和验证算法

- 加密算法
  - DES（56bit→64bit）
  - 3DES(3个 56bit →64bit）
  - AES (128、192、256)
  - 国密(256)
- 验证算法
  - MD5(128bit）
  - SHA-1(160bit）

计算复杂度与加密强度没必然联系

 Page 13



- **加密算法：**

  ESP能够对IP报文内容进行加密保护，防止报文内容在传输过程中被窥探。加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。

  一般来说IPSec使用加密算法有以下几种：

  - DES（Data Encryption Standard）

    使用56bit的密钥对一个64bit的明文块进行加密。

  - 3DES（Triple Data Encryption Standard）

    使用三个56bit的DES密钥（共168bit密钥）对明文进行加密。

  - AES（Advanced Encryption Standard）

    使用AES密钥对明文进行加密。密钥的长度分为128bit、192bit、256bit。

    3DES比DES具有更高的安全性，但其加密数据的速度要比DES慢得多。AES比3DES的计算复杂度低，而加密强度却比3DES高。

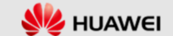
- **验证算法：**

  AH和ESP都能够对IP报文的完整性进行验证，以判别报文在传输过程中是否被篡改。验证算法的实现主要是通过杂凑函数，杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。

加密和验证算法

- 加密算法
  - DES（56bit→64bit）
  - 3DES(3个 56bit →64bit）
  - AES (128、192、256)
  - 国密(256)
- 验证算法
  - MD5(128bit）
  - SHA-1(160bit）

计算复杂度与加密强度没必然联系



一般来说IPSec使用两种验证算法：

- MD5（Message Digest 5）

  MD5通过输入任意长度的消息，产生128bit的消息摘要。

- SHA-1（Secure Hash Algorithm）

  SHA-1通过输入长度小于264bit的消息，产生160bit的消息摘要。

SHA-1的摘要长于MD5，因而是更安全的。但是SHA1的计算过程比MD5更耗费时间和资源。



目录





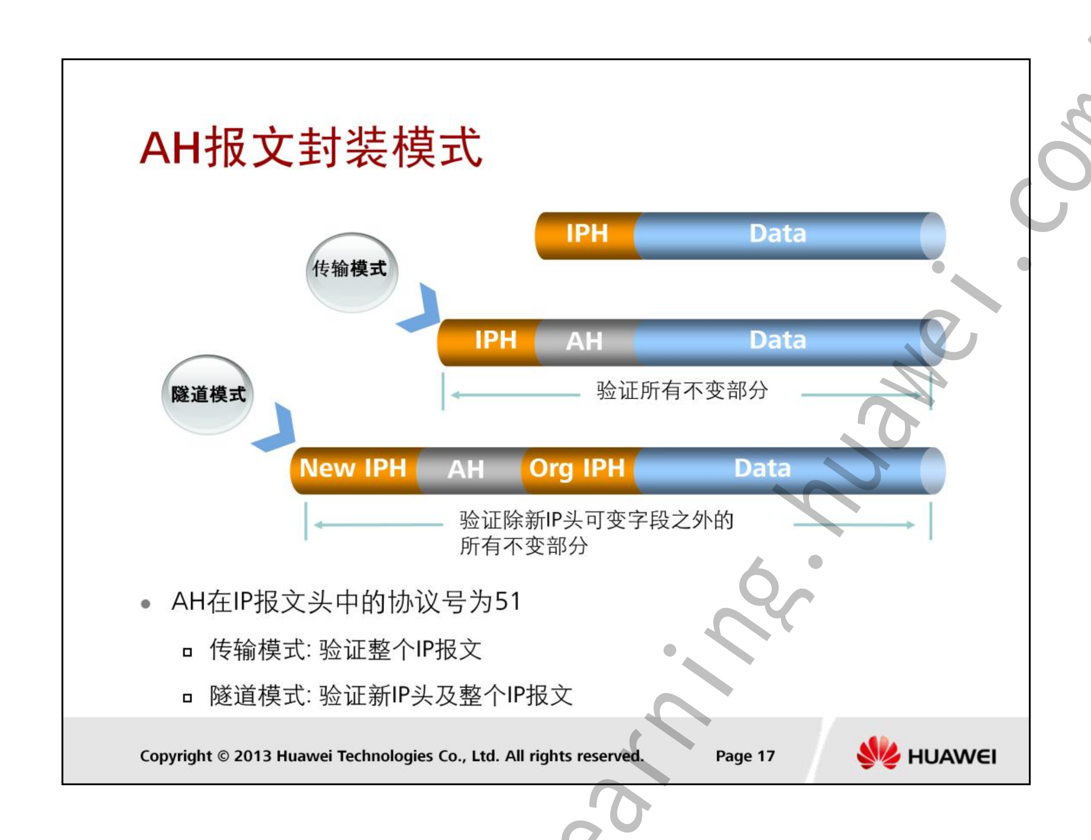
- IPSec协议组成——AH

验证头（Authentication Header，AH）是IPSec协议集合中的另外一个重要安全协议，用于为IP提供数据完整保护、数据原始身份认证以及防重放服务。它定义在RFC2402中。除了机密性之外，AH提供ESP能够提供的一切功能。

由于AH不提供机密性保证，所以它也不需要加密算法。AH定义保护方法、报头的位置、身份验证的覆盖范围以及输出和输入处理规则，但没有对所用的身份验证算法进行定义。与ESP一样，AH没有硬性规定防重放保护，是否使用防重放服务由接收端自行选择。发送端无法得知接收端是否会检查其序列号，其结果是，发送端必须一直认定接收端正在采用防重放服务。

和ESP一样，AH也是IP的一个万用型安全服务协议。但是AH提供的数据完整性与ESP提供的数据完整性稍有不同；AH对外部IP头各部分也会进行身份验证。

AH分配到的协议号是51。也就是说，使用AH协议进行安全保护的IPv4数据报文的IP头部中协议字段将是51，表明IP头之后是一个AH头。AH头比ESP头简单得多，因为它没有提供机密性。由于不需要填充和一个填充长度指示器，因此也不存在尾部字段。另外，也不需要一个初始化向量。



AH使用传输模式来保护一个上层协议，或者使用隧道模式来保护一个完整的IP数据报。在任何一种模式下， AH头都会紧跟在一个IP头之后。AH可以单独使用， 也可以与ESP联合使用，为数据提供最完整的安全保护。

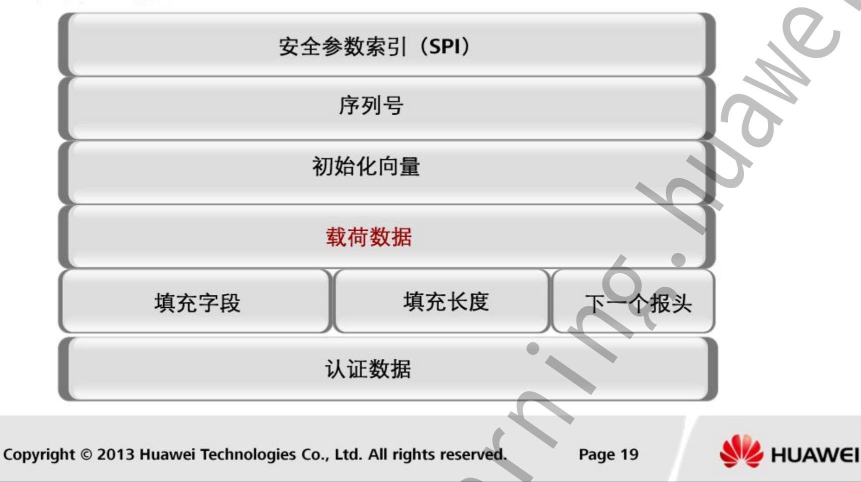
AH用于传输模式时，保护的是端到端的通信。通信的终点必须是IPSec终点。AH头被插在数据报中，紧跟在IP头之后（和任意选项），需要保护的上层协议之前。

AH用于隧道模式时，它将自己保护的数据报文封装起来，另外，在AH头之前，另添了一个新的IP头。 “里面的”IP数据报中包含了通信的原始报文，而新的IP头则包含了IPSec端点的地址。隧道模式可用来替换端对端安全服务的传输模式。



目录





- IPSec协议组成——ESP

ESP使用一系列加密算法提供机密性，数据完整性则由认证算法保证。具体使用过程中采用的算法则是由ESP安全联盟的相应组件决定的。另外ESP能够通过序列号提供防重放服务，至于是否采用则由数据包的接收者来决定。这是因为一个唯一的、单向递增的序列号是由发送端插入的，但却并不要求接收端对该数据报进行检验。由于这项保护对安全性大有好处，所以一般都会采用。

ESP可在不同的操作模式下使用。不管ESP处于什么模式， ESP头都会紧紧跟在一个IP头之后。在IPv4中，ESP头紧跟在IP头后面。ESP使用的协议号是50。也就是说，当ESP头插入原始报文中后，ESP之前的IP头中的协议字段将是50，以表明IP头之后是一个ESP头

作为一个IPSec头，ESP头中必然包含一个SPI字段。这个值，和IP头之前的目标地址以及协议结合在一起，用来标识特定的安全联盟。SPI本身是个任意数，可以是使用者自己指定，也可交由一些密钥管理技术自行协商决定。需要注意的是， SPI可以经过了验证，但却无法被加密。这是必不可少的一种做法，因为SPI用于SA的标识，指定了采用的加密算法以及密钥，并用于对包进行解密。如果SPI本身已被加了密，我们会碰到一个非常严重的问题——“先有鸡，还是先有蛋”。

序列号是一个独一无二、单向递增、并由发送端插在ESP头中的一个32位数值。通过序列号，ESP具有了防重放的能力。与SPI一样，序列号经过了验证，但却没有加密。这是由于我们希望在协议模块处理流程的最前端可以根据它判断一个包是否重复，然后决定是否丢弃这个包，而不至于动用更多的资源对其进行解密。

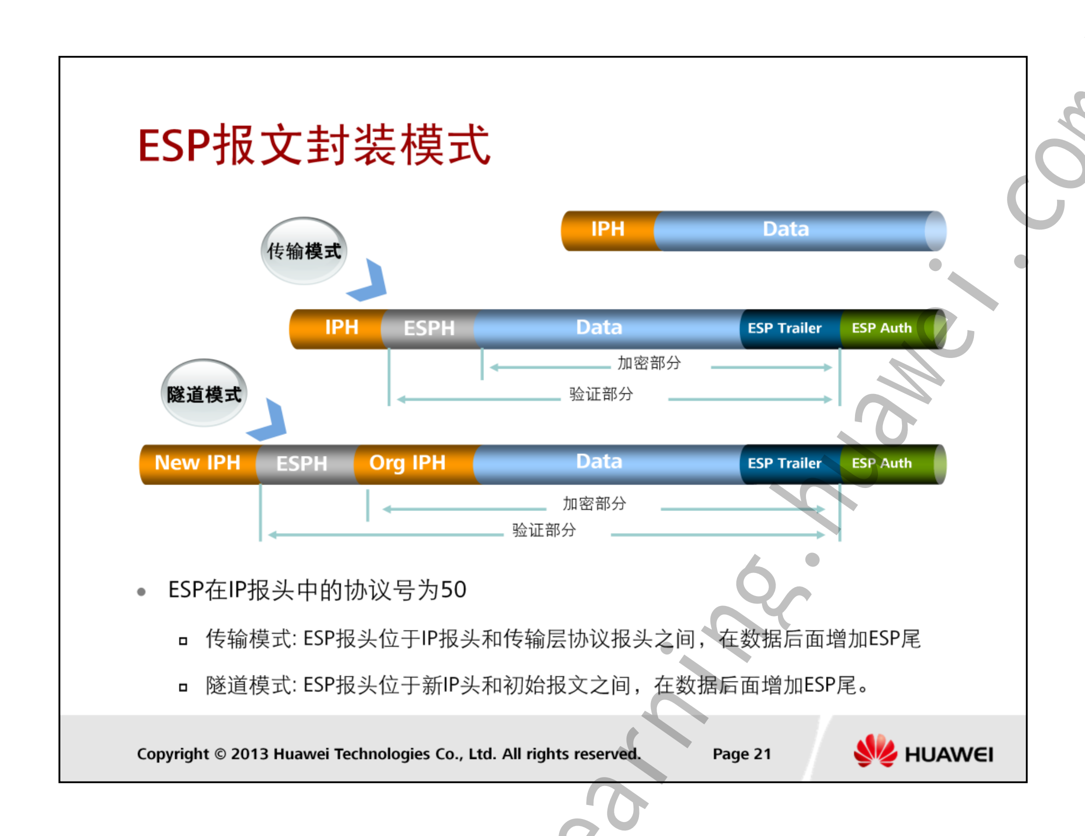
初始化向量（IV, Initial Vector）并不是一个必不可少的字段，但在ESP定义的加密算法中，有一些特殊的加密算法需要这个值。根据不同的加密算法，IV的取值方式也不尽相同。以DES-CBC来说，IV是载荷数据字段中的第一个8位组。相同的原因，IV也是只验证不加密的字段。

填充字段在ESP头中主要有三个功能。某些加密算法对输入的明文有严格的定义，例如明文的大小必须是某个数目字节的整数倍(如分块加密算法中要求明文是单块长度的整数倍）。填充字段的第一个功能就是将明文扩展到算法需要的长度。另外，由于ESP要求ESP头必须是32比特的整数倍，“填充长度”以及“下一个报头”这两个字段需要靠右对齐排列，填充字段也用来保证这样的报文格式。最后一个功能是处于安全性考虑的，就是填充字段可以隐藏数据载荷的实际长度，从而提供一定的保密性。填充字段的最大长度可达255个字节。填充内容与提供机密性的加密算法有关，如果这个算法定义了一个特定值，那么填充字段的内容就只能采用这个值。如果算法没有指定需要填充的值，ESP就会指定填充的第一个字节的值是1，后面的所有字节值都单向递增。

填充长度字段则标明了“填充字段”中填充数据的长度。接收端可以根据这个字段恢复载荷数据的真实长度。填充项长度字段是硬性规定的，因此，即使没有填充，填充长度字段仍会将它表示出来。

下一个报头字段表明载荷内的数据类型。如果在隧道模式下使用ESP，这个值就会是4，表示IP-in-IP。如果在传输模式下使用ESP，这个值表示的就是它背后的上一级协议的类型，比如TCP对应的就是6。

认证数据字段用于容纳数据完整性的检验结果，通常是一个经过密钥处理的散列函数。这一字段的长度由SA所用的身份验证算法决定。如果 SA中没有指定认证算法，则认证数据字段将不存在。

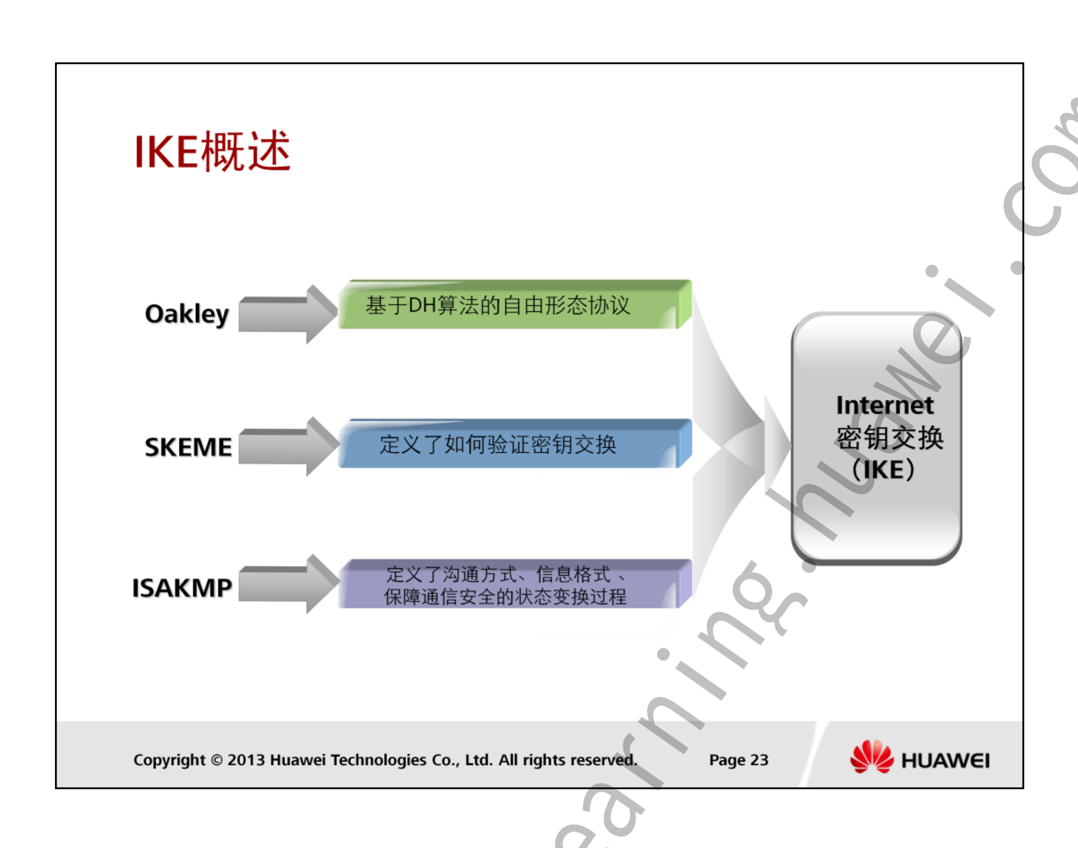


具体应用中，ESP可以使用传输模式也可以使用隧道模式。不同的模式决定了ESP对保护对象的定义。在传输模式中无法保护原有的IP头；在隧道模式中，整个原始报文都可以受到保护。



目录





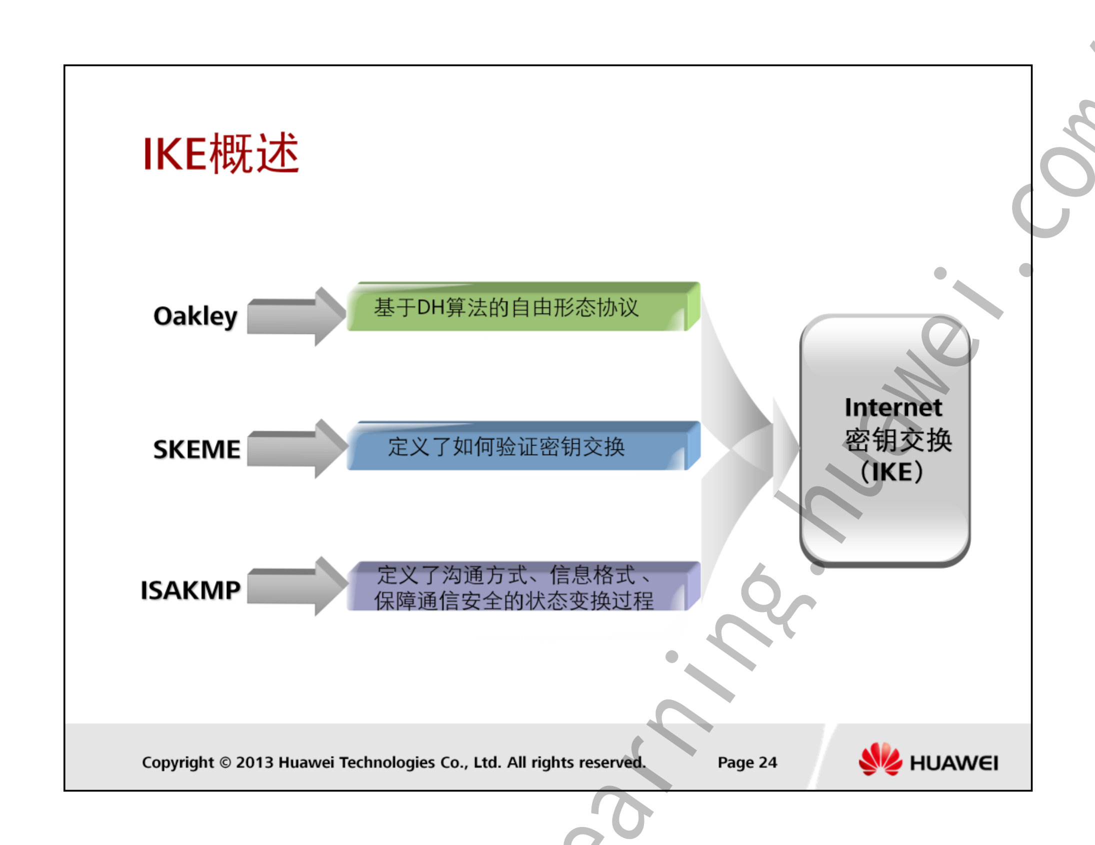
用IPSec保护一个IP包之前，必须先建立一个安全联盟（SA）。IPSec的安全联盟可以通过手工配置的方式建立。但是当网络中节点较多时，手工配置将非常困难，而且难以保证安全性。这时就可以使用IKE（Internet Key Exchange）自动进行安全联盟建立与密钥交换的过程。Internet密钥交换（IKE）就用于动态建立SA，代表IPSec对SA进行协商。

由RFC2409文件描述的IKE属于一种混合型协议。它建立在由Internet安全联盟和密钥管理协议（ISAKMP）定义的一个框架上，详情可见RFC2408文件。同时，IKE还实现了两种密钥管理协议的一部分——Oakley和SKEME。此外，IKE还定义了它自己的两种密钥交换方式。

Oakley是由亚利桑那大学的安全专家Hilarie Orman开发的一种基于Diffie-Hellman（简称“DH”）算法的协议。它是一种自由形态的协议，允许各研究机构根据自身的水平改进协议状态。IKE在其基础上定义了正规的密钥交换方法。尽管由于降低了Oakley模型的灵活性，但仍然提供了多种交换模式供用户选择，所以最终还是成为一个非常适宜的密钥交换技术。

SKEME则是另外一种密钥交换协议，由加密专家Hugo Krawczyk设计。SKEME定义了如何验证密钥交换。其中，通信各方利用公共密钥加密实现相互间的验证，同时“共享”交换的组件。每一方都要用对方的公共密钥来加密一个随机数字，两个随机数（解密后）都会对最终的密钥产生影响。IKE在它的一种验证方法（公共密钥加密验证）中，直接借用了SKEME的这种技术。

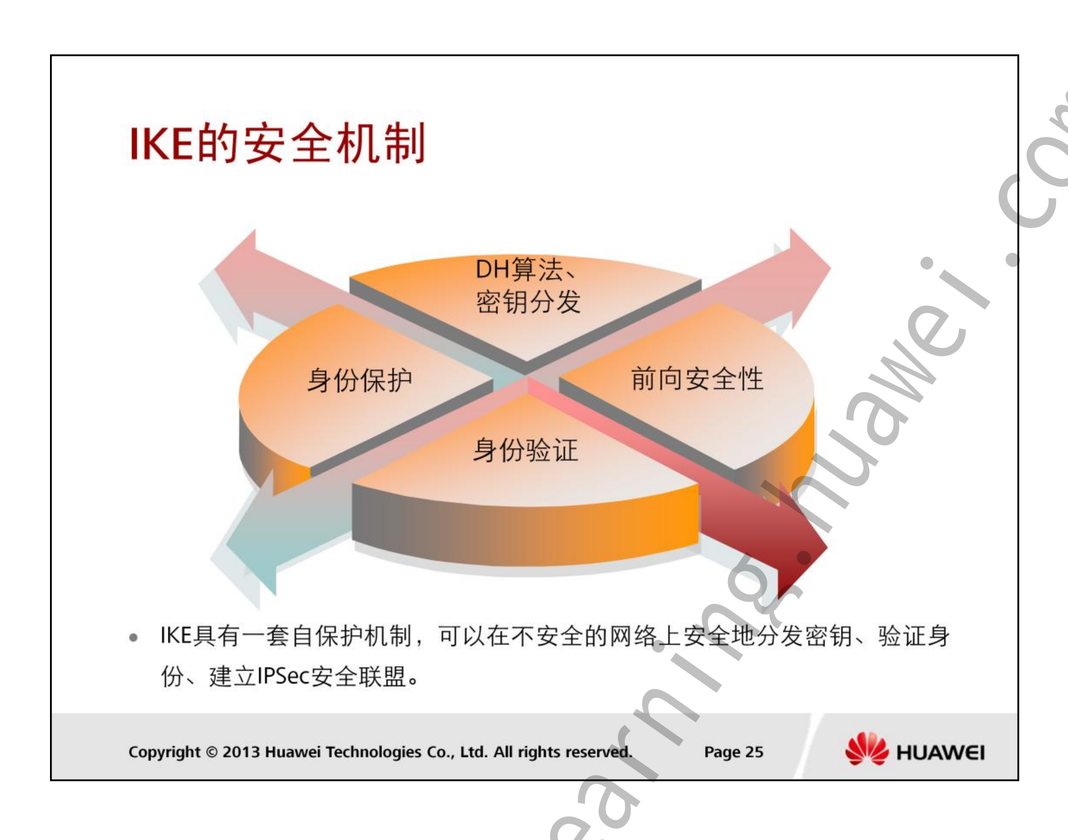
ISAKMP是由美国国家安全局（NSA）的研究人员开发出来的。NSA过去是一个高度机密的组织，美国政府甚至还否认过它的存在。近年来， NSA已慢慢走到公众面前，其专



业加密技术和安全技术也日渐引人瞩目。ISAKMP便是由它公开的一项技术。

ISAKMP、Oakley和SKEME—这三个协议构成了IKE的基础。因此，我们说IKE是一种“混合型”协议，它沿用了ISAKMP的基础、Oakley的模式以及SKEME的共享和密钥更新技术，从而定义出自己独一无二的验证加密材料生成技术，以及协商共享策略。在IKE规范中，三种技术发挥的作用可在后文对IKE本身的讨论中略见一二，其中ISAKMP发挥的作用最为巨大。

ISAKMP定义了通信双方沟通的方式，信息的格式以及定义了保障通信安全的状态变换过程。 但ISAKMP本身没有定义具体的密钥交换技术。密钥交换的定义留给其他协议处理。对IPSec而言，已定义的密钥交换就是IKE——即Internet密钥交换。IKE利用ISAKMP语言来定义密钥交换，是对安全服务进行协商的手段。IKE交换的最终结果是一个通过验证的密钥以及建立在双方同意基础上的安全服务——亦即所谓的“IPSec安全联盟（IPSec SA）”。但是， IKE并非仅由IPSec专用的。只要其他协议需要，比方说RIPv2或OSPF，也可以使用它来提供安全服务。



IKE具有一套自保护机制，可以在不安全的网络上安全地分发密钥、验证身份、建立IPSec 安全联盟。

- DH（Diffie-Hellman）交换及密钥分发

Diffie-Hellman 算法是一种公共密钥算法。通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥。加密的前提是交换加密数据的双方必须要有共享的密钥。IKE 的精髓就在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥。即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。

- 完善的前向安全性（Perfect Forward Secrecy）

PFS 是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。PFS 是由DH 算法保障的。此特性是通过在IKE 阶段2的协商中增加密钥交换来实现的。

- 身份验证

身份验证确认通信双方的身份。对于pre-shared key 验证方法，验证字用来作为一个输入产生密钥，验证字不同是不可能在双方产生相同的密钥的。验证字是验证双方身份的关键。

- 身份保护

身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

IKE在IPSec协议的作用

- 降低手工配置的复杂度
- 安全联盟定时更新
- 密钥定时更新
- 允许IPSec提供反重放服务
- 允许在端与端之间动态认证



 Page 26



IKE协议中的DH交换过程，每次的计算和产生结果都是毫无关系的。为保证每个安全联盟所使用的密钥互不相关，必须每次安全联盟的建立都运行DH交换过程。

IPSec使用IP报文头中的序列号实现防重放。此序列号是一个32比特的值，此数溢出后，为实现防重放，安全联盟需要重新建立，这个过程与要IKE协议的配合。

对安全通信的各方身份的的验证和管理，将影响到IPSec的部署。IPSec的大规模使用，必须有CA-Certification Authority（认证中心）或其他集中管理身份数据的机构的参与。

安全联盟（Security Association）

- 定义：
  - SA是通信对等体间对某些要素的约定，通信的双方符合SA约定的内容，就可以建立SA。
- SA由三元组来唯一标识，包括：

安全参数索引　　目的IP地址　　安全协议号

 Page 27



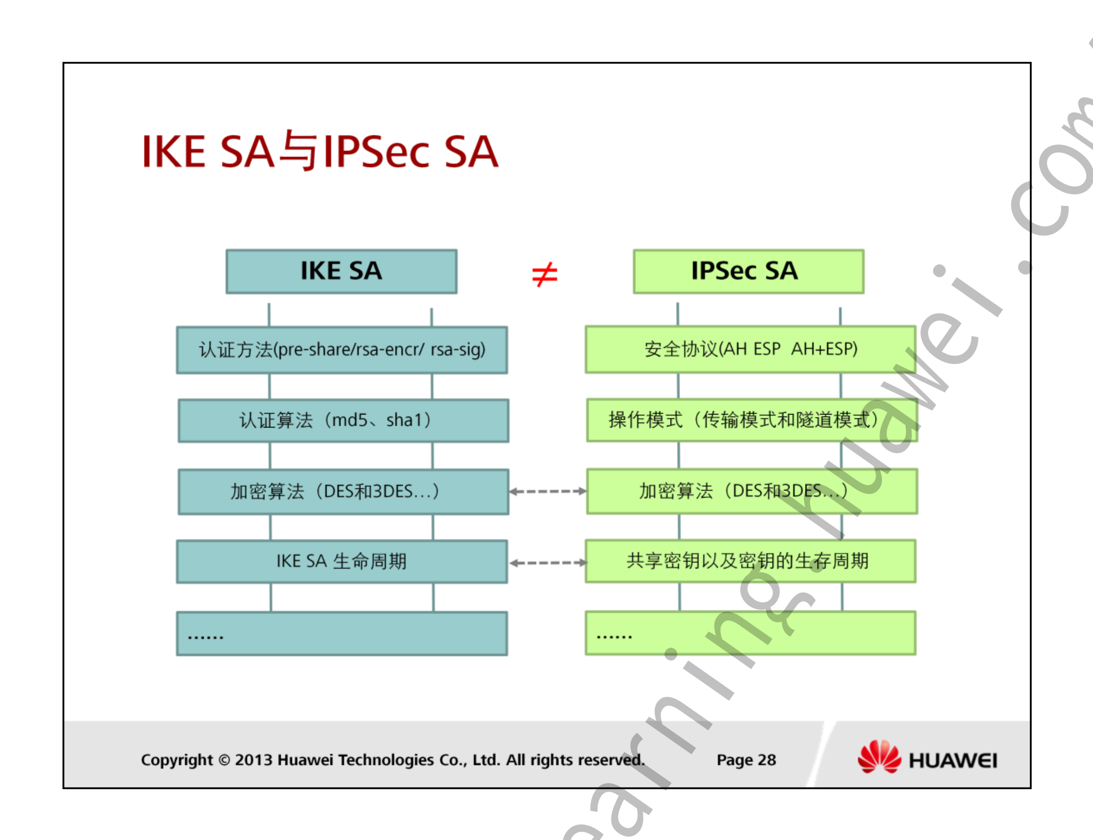
IPSec是在两个端点之间提供安全通信，端点被称为IPSec对等体。IPSec能够允许系统、网络的用户或管理员控制对等体间安全服务的粒度。例如，某个组织的安全策略可能规定来自特定子网的数据流应同时使用AH和ESP进行保护，并使用3DES（Triple Data Encryption Standard）进行加密；另一方面，策略可能规定来自另一个站点的数据流只使用ESP保护，并仅使用DES加密。通过SA（SecurityAssociation），IPSec能够对不同的数据流提供不同级别的安全保护。

安全联盟是IPSec的基础，也是IPSec的本质。SA是通信对等体间对某些要素的约定，例如，使用哪种安全协议、协议的操作模式（传输模式和隧道模式）、加密算法（DES和3DES）、特定流中保护数据的共享密钥以及密钥的生存周期等。

安全联盟是单向的，在两个对等体之间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。入站数据流和出站数据流分别由入站SA和出站SA进行处理。同时，如果希望同时使用AH和ESP来保护对等体间的数据流，则分别需要两个SA，一个用于AH，另一个用于ESP。

安全联盟由一个三元组来唯一标识，这个三元组包括安全参数索引（SPI，Security Parameter Index）、目的IP地址、安全协议号（AH 或ESP）。SPI 是为唯一标识SA而生成的一个32 比特的数值，它在IPSec头中传输。

IPSec设备会把SA的相关参数放入SPD（Security Policy Database）里面，SPD里面存放着“什么数据应该进行怎样的处理”这样的消息，在IPSec数据包出站和入站的时候会首先从SPD数据库中查找相关信息并做下一步处理。



从协商的内容上来看，由于IKE SA的主要作用是为IPSec SA协商出所使用的安全协议，因此IKE SA的主要协商内容为AH或ESP协议所使用的认证算法和加密算法，以及IPSec所使用的认证方法。

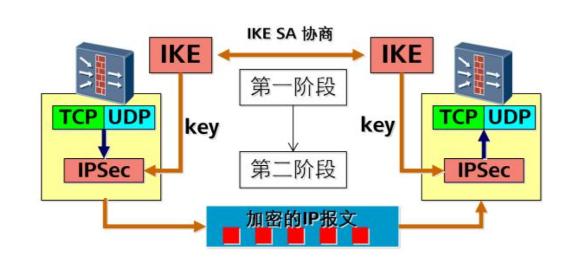
IPSec SA是要建立IPSec隧道的通信双方对隧道参数的约定，包括隧道两端的IP地址，隧道采用的验证方式、验证算法、验证密钥、加密算法、加密密钥、共享密钥以及生存周期等一系列参数。

IKE经过两个阶段为IPSec进行密钥协商并建立安全联盟：

第一阶段交换，通信各方彼此间建立了一个已通过身份验证和安全保护的通道，此阶段的交换建立了一个ISAKMP安全联盟，即ISAKMP SA（也可称为IKE SA）。

第二阶段交换，用已经建立的安全联盟（IKE SA）为IPSec协商安全服务，即为IPSec协商具体的安全联盟，建立IPSec SA，IPSec SA用于最终的IP数据安全传送。

IKE的交换阶段



- IKE使用了两个阶段为IPSec进行密钥协商并建立安全联盟：
  - 第一阶段，通信各方彼此间建立了一个已通过身份验证和安全保护的隧道，即IKE SA。协商模式包括主模式、野蛮模式。认证方式包括预共享密钥、数字签名方式、公钥加密。
  - 第二阶段，用在第一阶段建立的安全隧道为IPSec协商安全服务，建立IPSec SA。IPSec SA用于最终的IP数据安全传送。协商模式为快速模式。

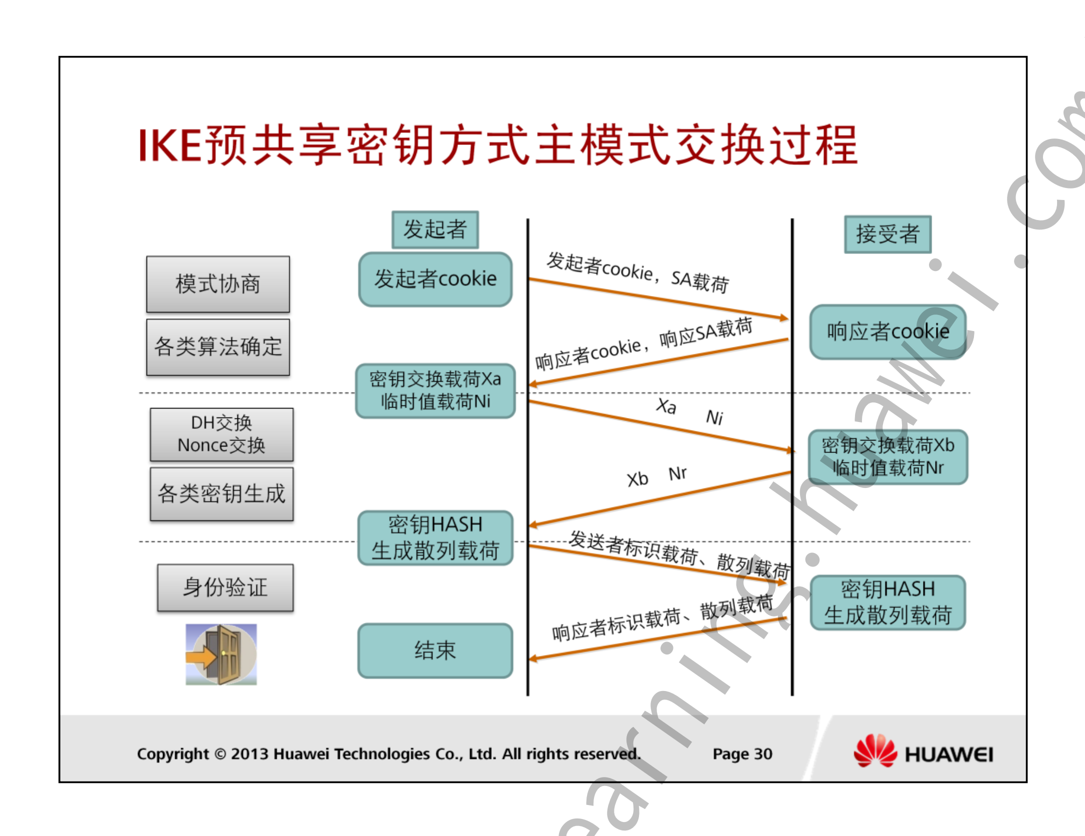
 Page 29 

IKE使用了两个阶段的ISAKMP。第一阶段建立IKE安全联盟（IKE SA），第二阶段利用这个既定的安全联盟，为IPSec协商具体的安全联盟。

在RFC2409（The Internet Key Exchange）中规定，IKE 第一阶段的协商可以采用两种模式：主模式（Main Mode）和野蛮模式（Aggressive Mode）。这两种模式各自做着相同的事情：建立一个加密和验证无误的通信信道（IKE SA），以及生成验证过的密钥，为双方的IKE通信提供机密性、消息完整性以及消息源验证服务。IKE中定义的其他所有交换都要求一个验证过的IKE SA作为首要条件。所以无论主模式还是野蛮模式，第一阶段都必须在其他任何交换之前完成。

IKE的工作流程如下：

1. 当一个报文从某接口外出时，如果此接口应用了IPSec，会进行安全策略的匹配。
2. 如果找到匹配的安全策略，会查找相应的安全联盟。如果安全联盟还没有建立，则触发IKE进行协商。IKE首先建立第一阶段的安全联盟，即IKE SA。
3. 在第一阶段安全联盟的保护下协商第二阶段的安全联盟，即IPSec SA。
4. 使用IPSec SA保护通讯数据。



主模式被设计成将密钥交换信息与身份认证信息相分离的一种交换技术。这种分离保证了身份信息在传输过程中的安全性，这是因为交换的身份信息受到了加密保护。

主模式总共需要经过三个步骤共6条消息来完成第一阶段的协商，最终建立IKE SA。

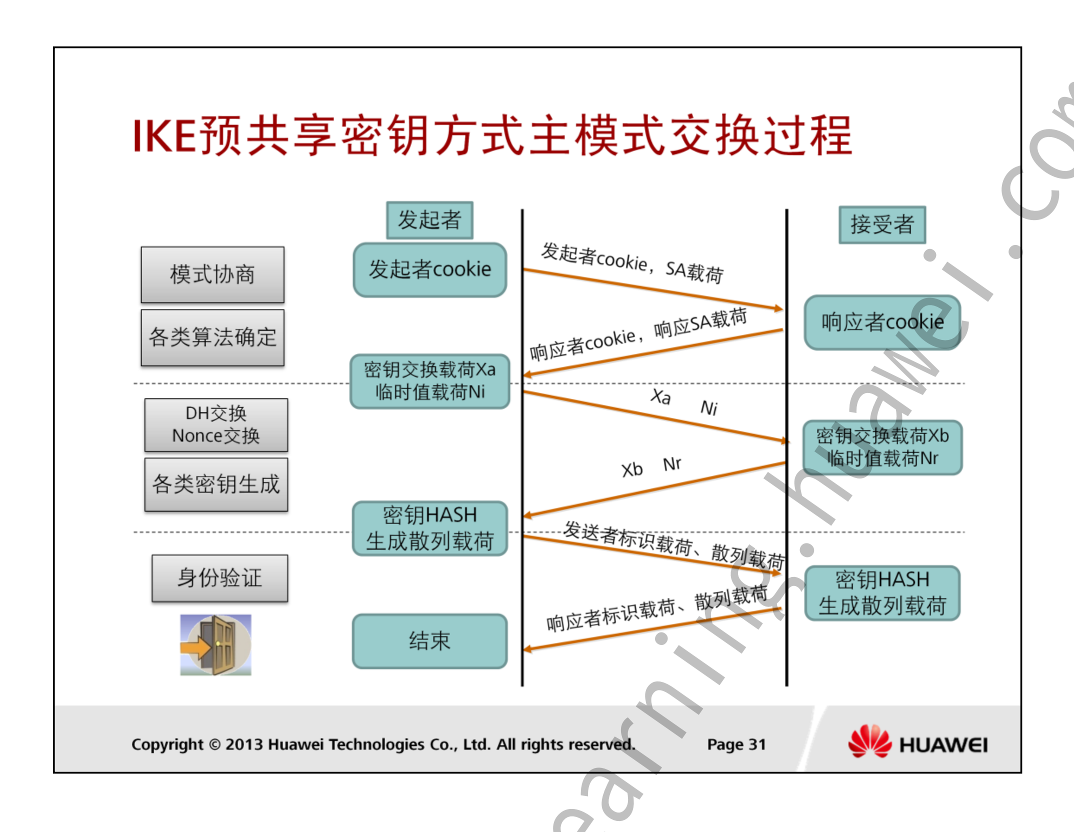
这三个步骤分别是模式协商、Diffie-Hellman交换和nonce交换、以及对对方身份的验证。主模式的特点包括身份保护以及对ISAKMP协商能力的完全利用。其中，身份保护在对方希望隐藏自己的身份时显得尤为重要。在我们讨论野蛮模式时，协商能力的完全利用与否也会凸显出其重要性。若使用预共享密钥方法验证。

在消息1、2发送之前，协商发起者和响应者必须计算产生自己的cookie，用于唯一标识每个单独的协商交换，cookie使用源/目的IP地址、随机数字、日期、和时间进行MD5运算得出，并且放入消息1的ISAKMP中，用以标识单独的一个协商交换。

在第一次交换中，需要交换双方的cookie和SA载荷，在SA载荷中携带需要协商的IKE SA的各项参数，主要包括IKE的散列类型、加密算法、认证算法和IKE SA的协商时间限制等。

第一次交换后第二次交换前，通信双方需要生成用于产生Diffie-Hellman共享密钥的DH值。生成方法是双方各自生成一个随机数字，通过DH算法对随机数字进行运算，得出一个DH值Xa和Xb（Xa是发起放的DH值，Xb是响应者的DH值），然后双方再根据DH算法运算得出一个临时值Ni和Nr。

第二次交换中，双方交换各自的密钥交换载荷（即Diffie-Hellman交换）以及临时值载荷（即nonce交换）。其中密钥交换载荷包含了Xa和Xb，临时值交换包含了Ni和Nr。

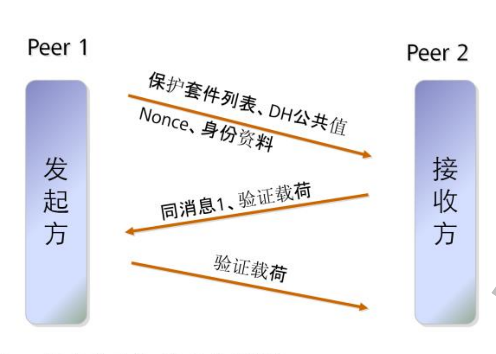


双方交换了临时值载荷Ni和Nr之后，配合事先预置好的预共享密钥，再通过为随机函数运算便可产生一个密钥SKEYID，这个密钥使后续所有密钥生成的基础。随后，通过自己算出来的DH值、交换得到的DH值以及SKEYID进行运算便可产生一个只有双方才知道的共享密钥SKEYID_d。此共享密钥并不进行传输，传输的只是是DH值以及临时值，因此即使第三方得到了这些材料也无法计算出共享密钥。

在第二次交换完成之后，双方所需的计算材料都已经交换完毕，此时，双方就可以将所有的密钥计算出来，并使用该密钥对随后的IKE消息提供安全保护。这些密钥包括：SKEYID_a以及SKEYID_e。SKEYID_a用来为IKE消息提供完整性以及数据源身份验证等安全服务；SKEYID_e则用于对IKE消息进行加密。

第三次交换是对标识载荷和散列载荷进行交换。标识载荷包含了发起者的标识信息、IP地址或主机名，散列载荷包含上一过程中产生的三组密钥进行HASH运算得出的值。这两个载荷通过SKEYID_e进行加密，如果双方的载荷相同，那么认证成功。IKE第一阶段主模式预共享密钥交换也就完成了。

IKE野蛮模式预共享密钥协商过程



- 野蛮模式一共需要交换3个消息
  - 消息1交换SA载荷、密钥材料、和身份信息
  - 消息2在交换消息1内容的同时增加了Hash认证载荷
  - 消息3是响应方对发起方的认证

 Page 32



- **IKE交换阶段第一阶段——野蛮模式交换**

从上述主模式协商的叙述中可以看到，在第二次交换之后便可生成会话密钥，会话密钥的生成材料中包含了预共享密钥。而当一个对等体同时与多个对等体进行协商SA时，则需要为每个对等体设置一个预共享密钥。为了对每个对等体正确地选择对应地预共享密钥，主模式需要根据前面交换信息中的IP地址来区分不同的对等体。

但是当发起者的IP地址是动态分配获得的时候，由于发起者的IP地址不可能被响应者提前知道，而且双方都打算采用预共享密钥验证方法，此时响应者就无法根据IP地址选择对应地预共享密钥。野蛮模式就是被用于解决这个矛盾的。

与主模式不同，野蛮模式仅用3条信息便完成了IKE SA的建立。由于对消息数进行了限制，野蛮模式同时也限制了它的协商能力，而且不会提供身份保护。

在野蛮模式的交换过程中，发起者会提供一个保护套件列表、Diffie-Hellman公共值、nonce以及身份资料。所有这些信息都是随第一条信息进行交换的。作为响应者，则需要回应选择一个保护套件、Diffie-Hellman公共值、nonce、身份资料以及一个验证载荷。发起者将它的验证载荷在最后一条消息交换。

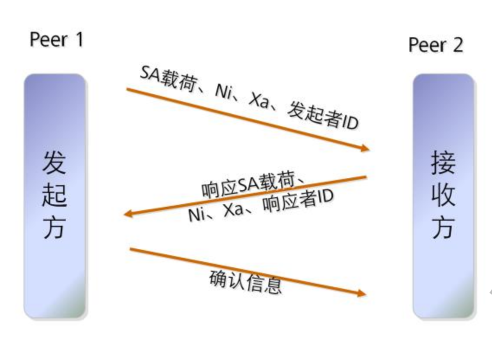
野蛮模式由于在其第一条信息中就携带了身份信息，因此本身无法对身份信息进行加密保护，这就降低了协商的安全性，但也因此不依赖IP地址标识身份，在野蛮模式下也就有了更多灵活的应用。

IKE主模式和野蛮模式区别

- 交换的消息:
  - 主模式为6个，野蛮模式为3个。
- 身份保护:
  - 主模式的最后两条消息有加密，可以提供身份保护功能；而野蛮模式消息集成度过高，因此无身份保护功能
- 对等体标识:
  - 主模式只能采用IP地址方式标识对等体；而野蛮模式可以采用IP地址方式或者Name方式标识对等体。



快速模式协商过程



- 快速模式一共需要交换3个消息
  - 消息1和消息2中，交换SA、KEY、Nonce和ID。用以协商算法、保证PFS以及提供“在场证据”
  - 消息3是用于验证响应者是否可以通信，相当于确认信息。

 Page 34 

- **IKE交换阶段第二阶段——快速模式交换**

建立好IKE SA之后（无论通过主模式还是通过野蛮模式交换），便可用它为IPSec生成相应的SA。IPSec SA是通过快速模式交换来建立的，对快速模式交换来说，它是在以前建立好的IKE SA的保护下完成的。

在一次快速交换模式中，通信双方需要协商拟定IPSec安全联盟的各项特征，并为其生成密钥。IKE SA保护快速模式交换的方法是：对其进行加密，并对消息进行验证。消息的验证是通过伪随机函数来进行的。来自IKE SA的SKEYID_a的值作为一个密钥，对快速模式交换的整个消息进行验证。这种验证除了能提供数据完整性保证之外，还能对数据源的身份进行验证：在消息接收到之后，我们知道它只有可能来自验证通过的实体，而且那条消息在传送过程并未发生改变。而通过加密（使用SKEYID_e），则可保障交换的机密性。

快速模式需要从SKEYID_d状态中衍生出用于IPSec SA的密钥。随同交换的nonce以及来自IPSec SA的SPI及协议一道，这个密钥将在伪随机函数中使用，这样便可确保每个SA都有自己独一无二的密钥：每个SA都有一个不同的SPI，所以入方向SA的密钥也会与出方向SA不同。所有IPSec密钥都是自相同的来源衍生的，所以相互间都有关联。假如一名攻击者能够根据IKE SA判断出SKEYID_d的值，那么就能非常容易地掌握自那个SKEYID_d衍生出来的任何IPSec SA的任何密钥。另外，还能继续掌握未来将要衍生的所有密钥！这显然是个大问题，所有这些密钥都不能保证所谓的“完美向前保密（PFS）”。快速模式为此专门提供了一个PFS选项，来满足这方面的需要，用户可根据自己地安全需要选择是否使用PFS。

为了在快速模式交换中实现PFS，需要执行一次额外的Diffie-Hellman交换，最终生成的共享密钥将在为IPSec生成密钥的过程中用到。显然，一旦交换完成，这个密钥便不复存在。一旦完成，它所驻留的那个内存位置必须清零和释放。从而保证了密钥之间地不相关性。

我们前面将快速模式描述成一种简单的请求／响应交换，但它的实际功用远不止于此。发起者可能需要一个“在场”证据，证明响应者在线，而且已经实际地处理了它的初始快速模式消息。为了达到这个要求，响应者需亚在验证散列载荷中，加入交换的发起者nonce以及消息ID。这个摘要现在不仅能保障消息的完整性，也能为发起者提供源验证功能，另外还能提供在场证据。

响应者也需要一个在场证据，从发起者传来的可能是一条过期的消息，是由不怀好意的人重播的。这个人可能不知道消息的内容，但通过对通信的分析，能够知道它是一条快速模式消息。如果重播那条消息，响应者便不得不创建多余的SA。我们可将其想像成一种“服务否认”攻击，只是属于比较温和的那种，因为响应者会根据这条消息，增加不必要的内存及SA管理开销。想要防范此类攻击，需在快速模式交换中增加第三条消息。在这条消息中，发起者需要同时包括nonce和此次交换的消息ID，并把它们保存在一个验证散列载荷中。这样发起者便可向响应者证实：自己是此次交换的活动参与者。

在前两条消息中，发起者和响应者都发送了SA载荷，和主模式、野蛮模式一样，SA载荷是用来协商各种保护算法的。而Ni、Nr以及ID则是用来提供“在场证据”的。Xa以及Xb则是用来生成新的DH共享密钥，保证PFS的。Xa以及Xb将与IKE第一阶段生成的SKEYID_d、Ni、Nr以及SPI等信息共同生成最终用于IPSec加密的密钥。

最后发起者会发送一条确认信息，响应者收到该信息后就知道发起者已经收到了第二条消息。此时IKE第二阶段结束。

密钥保护

- 密钥生存周期
  - 密钥具有一定生存期，当生存期到达时，用新的密钥替代原有密钥；
- 完美向前保密（PFS）
  - 定义两个密钥之间无任何关系
- Diffie-Hellman(DH)组
  - 公共密钥加密系统，可在一个公共的、不受安全保护通讯信道（Internet）交换共享密钥生成过程信息；

 Page 36



- 密钥生存周期

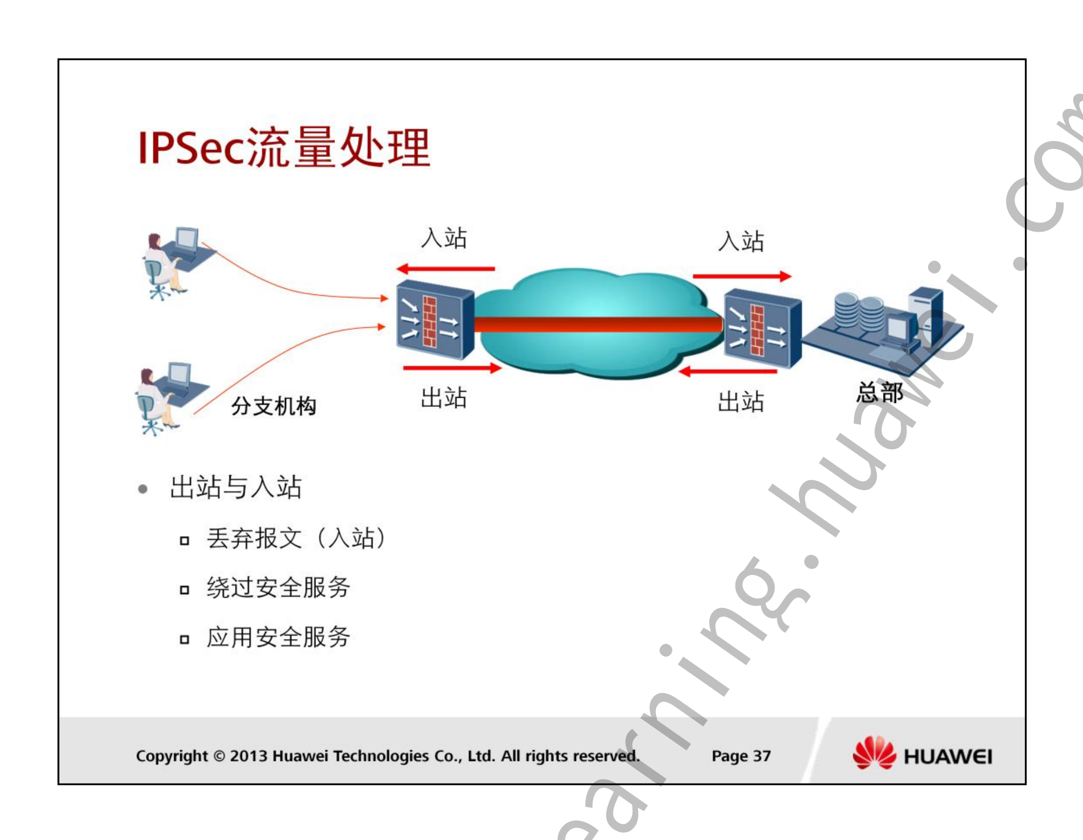
　　密钥生命周期设置决定何时把旧密钥替换成新密钥。密钥生命周期决定了在一定的时间段内，新旧密钥交替的周期。例如，在某业务通信中需要1000秒，而我们设定密钥生命周期为100秒，那么整个数据报文传输期间将会产生10个密钥。由于在此业务通信周期内使用了10个密钥，即使攻击者破解了某个密钥对数据报文进行解密处理，也无法实现对所有数据报文的解密。

- 完美向前保密（PFS）

　　完美向前保密，即每一密钥均是“独一无二”的，这样一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。所以若有攻击者破解了一个密钥后，只能访问受这个密钥保护的所有数据报文，而受其它密钥保护的数据报文还是无法破解。PFS是由DH算法保障的。此特性是通过在IKE阶段2的协商中增加密钥交换来实现的。

- Diffie-Hellman (DH) 组

　　DH算法是一种公共密钥算法。通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥。加密的前提是交换加密数据的双方必须要有共享的密钥。IKE的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥。即使第三方（如黑客）截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。IKE共定义了5个DH组，组1定义的密钥长度为768位；组2长度为1024位。密钥长度越长，所生成的密钥安全度也就越高，越难被破译。DH组的选择很重要，因为DH组只在第一阶段的SA协商中确定，第二阶段的协商不再重新选择DH组，两个阶段使用的是同一个DH组，因此该DH组的选择将影响所有“会话密钥”的生成。在协商过程中，对等的实体间应选择同一个DH组，即密钥长度应该相等。若DH组不匹配，将视为协商失败。



基于IPSec业务应用，不管是出站还是入站流量，防火墙均根据数据类型采取丢弃报文、绕过安全服务和应用安全服务等3方面进行处理。

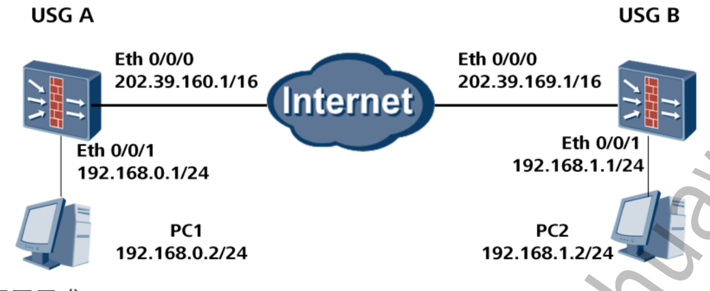
- 出站流量：防火墙首先查看出站数据报文流量是否属于定义的保护数据流，以判断将为这个报文提供哪些安全服务输出，可能有以下几类情况：
  - 绕过安全服务：在这类情况下，报文不属于定义的保护数据流，将不应用IPSec策略，只进行传统的IP转发处理流程；
  - 应用安全服务：在这类情况下，此报文将根据已建立的SA，对报文应用IPSec策略后进行转发。对于尚未建立SA情况，将调用IKE，以便完成SA建立；
- 入站流量：入站流量处理与出站流量有所区别，其将根据报文是否含有IPSec头对此报文进行以下动作处理。
  - 丢弃报文：若报文不含IPSec头，且查看防火墙安全转发策略后，其策略输出为丢弃，那么数据报文就会被丢弃。若策略输出为应用IPSec，但SA未建立数据报文同样也会被丢弃
  - 绕过安全服务：若报文不含IPSec头，则根据防火墙安全转发策略将数据报文进行传统的IP转发处理流程；
  - 应用安全服务：若报文含IPSec头，且已建立SA，那么数据报文将会被递交给IPSec层进行处理；



目录



点对点IPSec应用场景



- 组网需求
  - PC1与PC2之间进行安全通信，在FWA与FWB之间使用IKE自动协商建立安全通道。
  - 在FWA和FWB上均配置序列号为10的IKE提议。
  - 为使用pre-shared key验证方法的提议配置验证字。
  - FWA与FWB均为固定公网地址

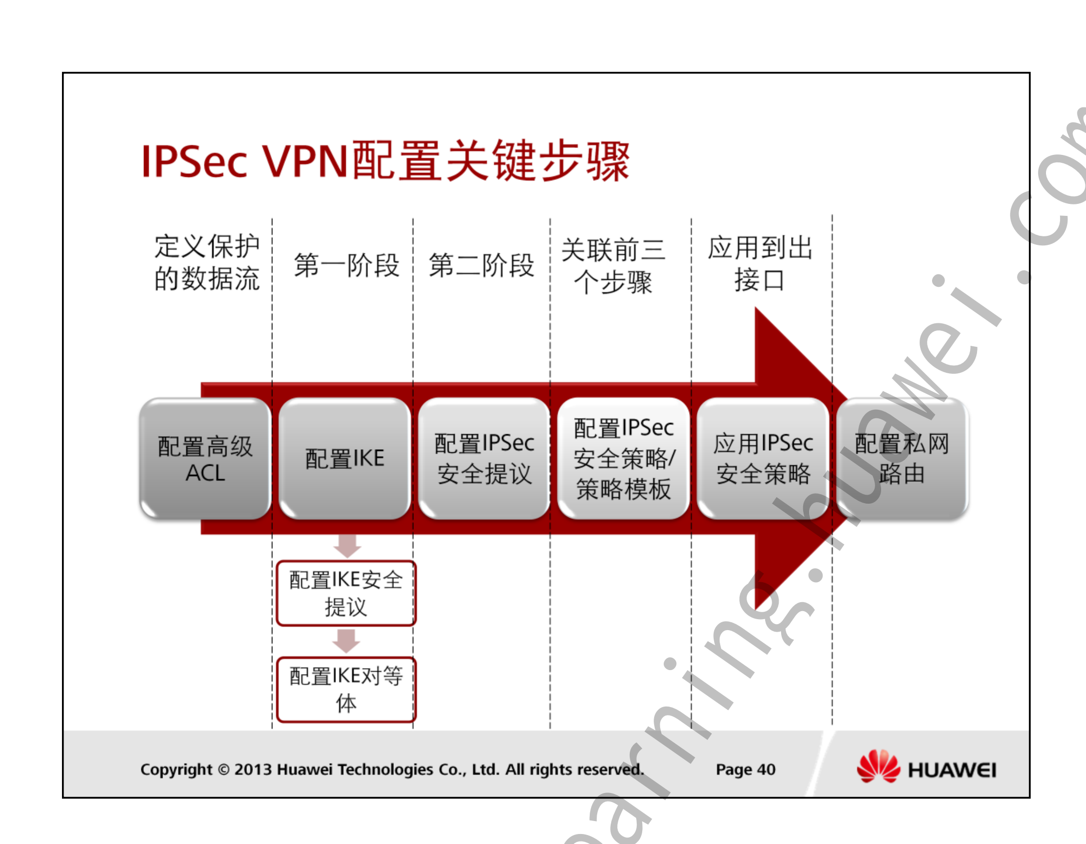
 Page 39



两个网络的公网IP地址固定不变，且两个网络之间要互相访问，可建立IKE协商的点到点方式的IPSec隧道，使两个网络中的设备都可以主动发起连接。

对于USG_A和USG_B，配置思路相同。如下：

1. 完成接口基本配置、路由配置，并开启本地策略和转发策略。
2. 配置IKE协商的第一阶段参数，包括IKE版本、协商模式、预共享密钥、对端IP地址等。
3. 在第一阶段基础上建立第二阶段。
4. 配置IPSec安全策略，添加需保护的数据流，即网络A和网络B两个网段的通信数据。
5. 将IPSec安全策略应用到接口上。


IPSec VPN配置关键步骤
定义保护的数据流
第一阶段
第二阶段
关联前三个步骤
应用到出接口
配置高级ACL
配置IKE
配置IPSec安全提议
配置IPSec安全策略/策略模板
应用IPSec安全策略
配置私网路由
配置IKE安全提议
配置IKE对等体
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 40
HUAWEI

步骤一：定义需要保护的数据流

- 配置高级ACL，定义需要保护的数据流

  [USG_A] acl 3000

  [USG_A-acl-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255

  [USG_B] acl 3000

  [USG_B-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.0 0.0.0.255

 Page 41



为不同方向、不同应用的数据流提供IPSec保护，使用ACL定义需要保护的数据流。数据流是一组流量（traffic）的集合，由源地址/掩码、目的地址/掩码、IP报文承载的协议号、源端口号、目的端口号等来规定。一个数据流由一个ACL来定义，所有匹配一个访问控制列表的流量，在逻辑上作为一个数据流。

IPSec使用高级ACL（Access Control List，访问控制列表）来定义需要保护的数据流。高级ACL的取值范围是3000-3999，通过源IP地址、目的IP地址、ToS、时间段、协议类型、优先级、ICMP报文类型和ICMP报文码等多个维度来对进行流量匹配，在大部分功能中都可使用高级ACL来进行精确流量匹配。

步骤二：配置IKE

- 创建IKE安全提议

  [USG_A] ike proposal 10

  [USG_A-ike-proposal-10] authentication-method pre-share

  [USG_A-ike-proposal-10] authentication-algorithm sha1

  [USG_A-ike-proposal-10] integrity-algorithm hmac-sha1-96

- 配置IKE对等体

  [USG_A] ike peer b

  [USG_A-ike-peer-b] ike-proposal 10

  [USG_A-ike-peer-b] remote-address 202.38.169.1

  [USG_A-ike-peer-b] pre-shared-key abcde



如果选择了pre-shared key验证方法，需要为每个对端配置预共享密钥。建立安全连接的两个对端的预共享密钥必须一致。

在野蛮模式下可以配置对端IP地址与对端名称，主模式下只能配置对端IP地址。缺省情况下，IKE协商采用主模式。

步骤三：IPSec安全提议配置

- 创建IPSec安全提议

```
[USG_A] ipsec proposal tran1
[USG_A-ipsec-proposal-tran1] encapsulation-mode tunnel
[USG_A-ipsec-proposal-tran1] transform esp
[USG_A-ipsec-proposal-tran1] esp authentication-algorithm md5
[USG_A-ipsec-proposal-tran1] esp encryption-algorithm des
```

- USG_B上的IPSec安全提议配置与USG_A相同

 Page 43



在配置IPSec安全提议时，可以只需要创建一个安全提议，其它参数采用缺省参数。缺省情况下，安全协议使用esp，AH和ESP协议采用的验证算法为MD5，ESP协议采用的加密算法为DES加密算法。

步骤四：配置IPSec安全策略

- 创建安全策略

[USG_A] ipsec policy map1 10 isakmp

[USG_A-ipsec-policy-isakmp-map1-10] security acl 3000

[USG_A-ipsec-policy-isakmp-map1-10] proposal tran1

[USG_A-ipsec-policy-isakmp-map1-10] ike-peer b

[USG_A-ipsec-policy-manual-map1-10] quit

[USG_B] ipsec policy map1 10 isakmp

[USG_B-ipsec-policy-isakmp-map1-10] security acl 3000

[USG_B-ipsec-policy-isakmp-map1-10] proposal tran1

[USG_B-ipsec-policy-isakmp-map1-10] ike-peer a

[USG_B-ipsec-policy-isakmp-map1-10] quit



步骤五：应用IPSec安全策略

- 分别在USG_A和USG_B的接口上引用各自的安全策略

```
[USG_A] interface GigabitEthernet 0/0/2
[USG_A-GigabitEthernet0/0/2] ipsec policy map1
[USG_B] interface GigabitEthernet 0/0/2
[USG_B-GigabitEthernet0/0/2] ipsec policy map1
```




Web方式步骤一：配置IKE

配置IKE peer，在防火墙B上的配置应与防火墙A对应。

配置IKE 对等体远端地址。

VPN > IPSec > IKE协商

新建阶段1

阶段1	ike_a *
版本	V1 / V2 / V1 and V2
协商模式	主模式 / 野蛮模式
本地ID类型	名称
远端名称	ike_peer_b *
本地名称	ike_peer_a *
预共享密钥	••••• *
对端网关配置方式	固定地址
对端网关VPN实例	public
对端网关IP	202 . 38 . 169 . 1 *
对端地址池范围	
VPN实例	public

高级

应用 返回

Page 46 HUAWEI

配置IKE阶段1和阶段2。

1. 选择“VPN > IPSec > IKE协商”。
2. 单击“阶段1”。
3. 在“新建阶段1”界面中，配置阶段1参数，如图所示。其中，“预共享密钥”设置为abcde。

在第一阶段，通信各方彼此间建立了一个已通过身份验证和安全保护的通道，此阶段的交换建立了一个ISAKMP安全联盟，即ISAKMP SA（也可称IKE SA）。在安全隧道的两端设置的安全协议、认证算法、加密算法、预共享密钥、完整性算法、DH组等必须相同，否则协商不能通过。

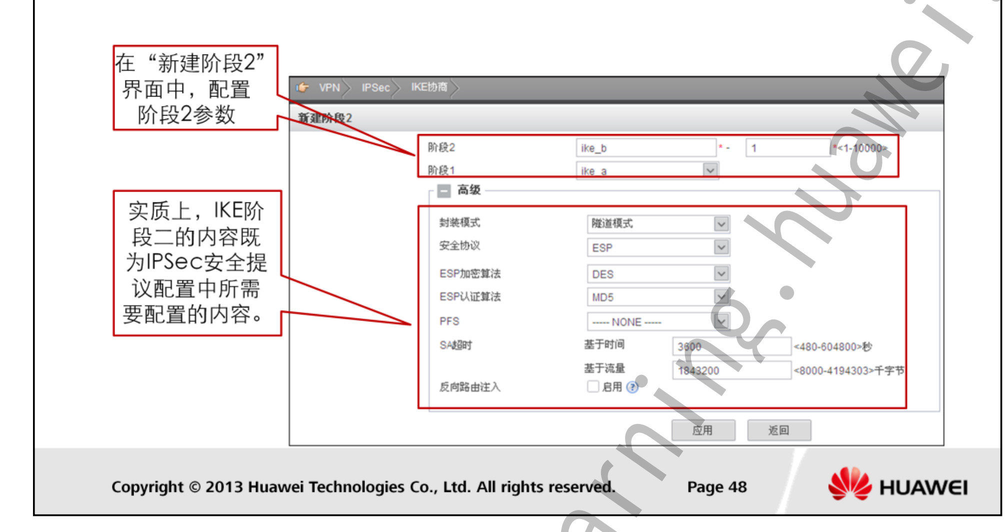
配置对端网关IP时，对端网关IP地址为对端网关建立隧道的接口的IP地址，即IPSec策略应用到的接口的IP地址。



在阶段一中的加密算法、认证算法、完整性算法等参数的缺省配置为图中所示。

Web方式步骤三：IPSec安全提议配置

- 在Web界面下，IPSec安全提议的配置在IKE第二阶段中实现。



在IKE第二阶段交换中，用已经建立的安全联盟（IKE SA）为IPSec协商安全服务，即为IPSec协商具体的安全联盟，建立IPSec SA。IPSec SA用于最终的IP数据安全传送。在第一阶段建立后，才能建立第二阶段，并对第一阶段进行引用。在安全隧道的两端设置的安全协议、报文封装模式、认证算法、加密算法、PFS等必须相同，否则协商不能通过。

Web方式步骤四：定义保护的数据流

HUAWEI

应用IPSec策略。

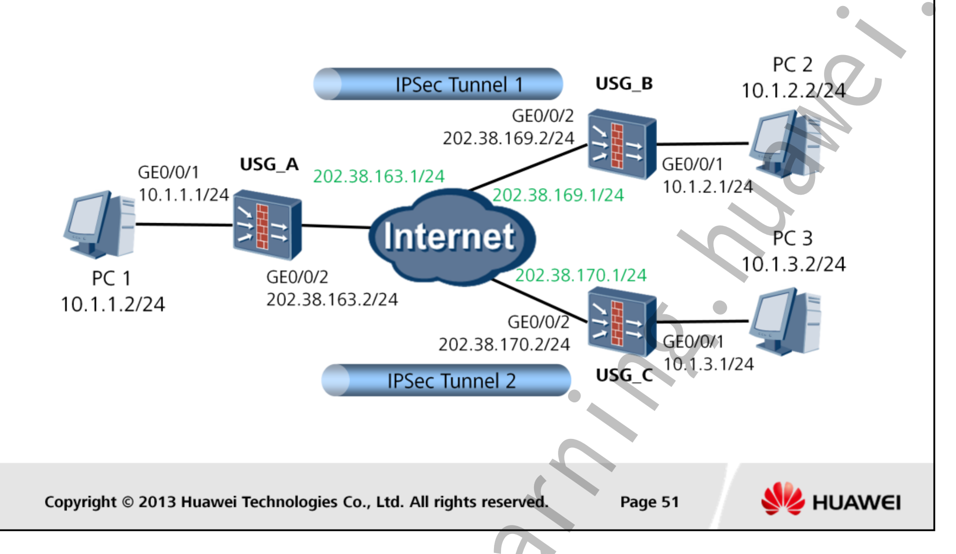
1. 选择“VPN > IPSec > IPSec策略”。
2. 单击“新建”。
3. 在“新建IPSec策略”界面中，配置IPSec策略参数

在命令行界面的配置中，首先使用ACL定义需要保护的数据流，然后再IPSec安全策略中应用该ACL。但在Web界面的配置中，可以直接在新建IPSec策略时指定需要保护的数据流。



将IPSec策略与接口绑定。

1. 选择“VPN > IPSec > IPSec策略”。
2. 单击“policy1”后的“应用接口：- NONE -”。
3. 在下拉列表中选择GE0/0/2。
4. 单击“应用”。



在实际的应用中，经常需要使用HUB-Spoke类型的组网，即一个总部到多个分支机构的组网，分支节点建立到总部的IPSec隧道，各个分支机构之间的通信由总部节点转发和控制。这样的应用场景，为点对多点的IPSec应用场景。

对于场景中的对于USG_A、USG_B和USG_C，配置思路相同。如下：

1. 完成接口基本配置、路由配置，并开启本地策略和转发策略。
2. 配置IKE协商的第一阶段参数，包括IKE版本、协商模式、预共享密钥、对端IP地址等。
3. 其中，USG_A不主动发起连接，不用指定对端网关IP地址。USG_B和USG_C需要指定对端网关IP地址为202.38.163.2/24。
4. 在第一阶段基础上建立第二阶段。
5. 配置IPSec安全策略，添加需保护的数据流，即总部、分支机构1和分支机构2网段的通信数据。
6. 将IPSec安全策略应用到接口上。

点到点与点到多点应用场景的配置比较类似，各分支机构的配置大致相同，他们的对端设备都应该为总部的USG防火墙。



进入Web配置页面，选择菜单栏中 “快速接入向导—>IPSec向导”，选择相应应用场景进行IPSec VPN配置；

1）选择应用场景；

2）配置网络：选择启用“IPSec应用”的网络口，且配置对端网关IP；

3）配置定义爱保护数据流；

4）配置加密与认证：一般情况下可采用默认配置，并保持两端配置统一；

IPSec结果验证与维护命令

- 查看到两条双向IPSec SA

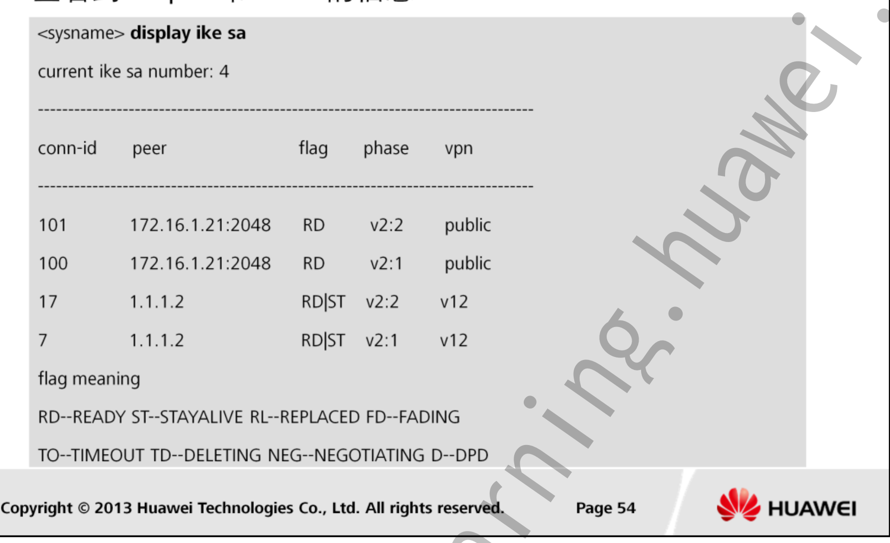
<FWA>display ipsec sa brief

```
current ipsec sa number: 2
----------------------------------------------------------------------------------------------
Src Address     Dst Address          SPI          VPN  Protocol  Algorithm
----------------------------------------------------------------------------------------------
202.39.160.1    202.39.169.1     957073432  0    ESP      E:DES;A:HMAC-MD5-96;
202.39.169.1    202.39.160.1    2838744079 0    ESP      E:DES;A:HMAC-MD5-96;
```


Page 53



PC1与PC2之间数据通信将触发IKE协商和IPSec VPN建立，成功建立VPN后，PC1与PC2之间进行可以相互访问.



IPSec结果验证与维护命令

- 查看到IKE peer和IKE sa的信息

```
<sysname> display ike sa
current ike sa number: 4
--------------------------------------------------------------------------------
conn-id    peer                 flag     phase    vpn
--------------------------------------------------------------------------------
101        172.16.1.21:2048     RD       v2:2     public
100        172.16.1.21:2048     RD       v2:1     public
17         1.1.1.2              RD|ST    v2:2     v12
7          1.1.1.2              RD|ST    v2:1     v12
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD--FADING
TO--TIMEOUT TD--DELETING NEG--NEGOTIATING D--DPD
```

 Page 54 HUAWEI

display ike sa命令可以查看到的信息包括：安全通道的标识符、安全联盟的对端IP地址、VPN实例名称、SA所属阶段、SA所属解释域、此安全联盟的状态。

在参数中，Peer表示此安全联盟的对端的IP地址。Phase表示此SA所属阶段，具体说明如下：

- Phase 1：建立安全通道进行通信的阶段，此阶段建立ISAKMP SA；
- Phase 2：协商安全服务的阶段，此阶段建立IPSec SA。

Flag显示此安全联盟的状态，其中：

- RD（READY）：表示此SA已建立成功；
- ST（STAYALIVE）：表示此端是通道协商发起方；
- RL（REPLACED）：表示此通道已经被新的通道代替，一段时间后将被删除；
- FD（FADING）：表示此通道已发生过一次软超时，目前还在使用，在硬超时时会删除此通道；
- TO（TIMEOUT）：表示此SA在上次keepalive超时发生后还没有收到keepalive报文，如果在下次keepalive超时发生时仍没有收到keepalive报文，此SA将被删除。
- TD（DELETING）：表示该条SA即将被删除。
- NEG（NEGOTIATING）：表示IKE SA正在协商中，是由隧道两端设置的某些参数不一致导致。
- D（DPD）：表示开启了DPD检测功能，并正在做DPD检测。

IPSec VPN配置注意事项

- 防火墙上必须有到达对方私网网段的正确路由
- USG2100连接内网的接口需要取消接口快转功能
- 主动触发IPSec VPN的防火墙ACL中必须定义Source字段,推荐双方的ACL的互为镜像
- 配置Local和Untrust域间缺省包过滤规则的目的为允许IPSec隧道两端设备通信，使其能够协商SA

 Page 55



IPSec 常见问题定位:

1. IKE第一阶段没有成功。

   使用display ike peer和display ike proposal检查隧道两端ike peer和ike proposal配置是否一致。

2. IKE第二阶段没有成功。

   一般问题都出在ACL上，确认被引用的ACL是否已经被匹配到。

   服务器端模板方式下，客户端ACL必须指定源IP所在网段。

   隧道中间是否存在NAT设备，是否配置了NAT穿越。

3. IPSec SA创建没有成功。

   检查IPSec proposal配置是否一致。

4. IPSec SA已经建立但是业务不通。



总结

- IPSec技术的基本原理
- AH和ESP技术
- IKE协议的业务流程
- IPSec VPN的应用场景及配置



思考题

- IPSec VPN可提供哪些安全服务？每个安全服务的意义和实现方式是什么？
- IPSec的2个主要安全协议是什么？它们之间有什么区别？
- IPSec的2个主要封装模式是什么？它们之间应用场景有何区别？
- IKE可提供哪4个安全机制？每个安全机制的作用各是什么？
- 安全联盟SA在IPSec中有何重要作用？它是通过哪三元组进行唯一标识？
- IKE第一阶段协商有哪2种模式？它们之间主要应用在什么场景下？
- IKE第一阶段协商2种模式的配置选项有什么不同？
- IPSec是采用什么技术触发IPSec隧道的建立？
- 在隧道模式下，如何配置私有网络路由？
- IPSec应用场景下，域间包过滤如何设置才能符合最小权限要求？请从业务流流向进行分析。



Thank you

www.huawei.com

HC110310010

HCNA-Security-CBSN 第十章 SSL VPN 技术

第十章

SSL VPN技术

www.huawei.com

HUAWEI



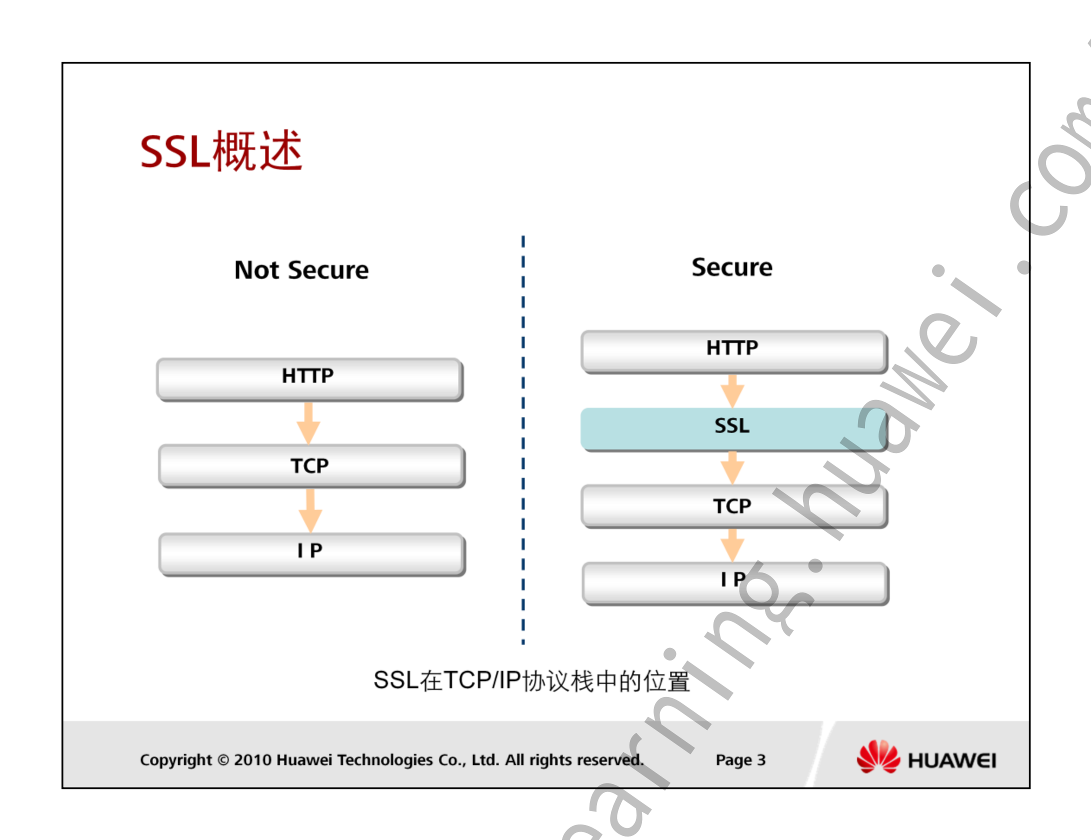
- 学完本课程后，您将能够:
  - 了解SSL VPN的技术原理
  - 熟悉SVN产品的基本功能和特性
  - 掌握SSL VPN配置方法





目录





SSL在TCP/IP协议栈中的位置

SSL是一个安全协议，为基于TCP（Transmission Control Protocol）的应用层协议提供安全连接，SSL介于TCP/IP协议栈第四层和第七层之间。SSL可以为HTTP（Hypertext Transfer Protocol）协议提供安全连接。SSL协议广泛应用于电子商务、网上银行等领域，为网络上数据的传输提供安全性保证。

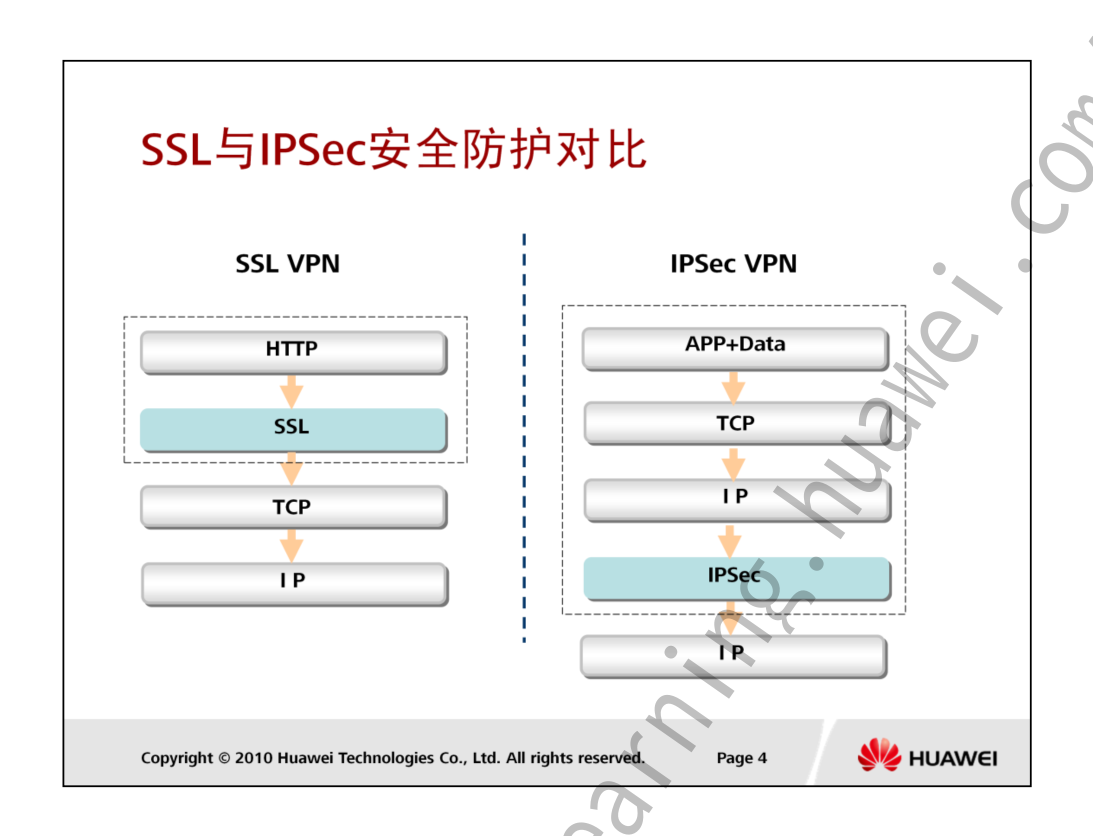
安全套接层(SSL)是一种在两台机器之间提供安全通道的协议。它具有保护传输数据以及识别通信机器的功能。

到目前为止，SSL协议有三个版本，其中SSL2.0和SSL3.0得到广泛的应用，IETF基于SSL3.0推出了TLS1.0协议(也被成为SSL3.1)。随着SSL协议的不断完善，包括微软IE在内的愈来愈多的浏览器支持SSL，SSL协议成为应用最广泛的安全协议之一。

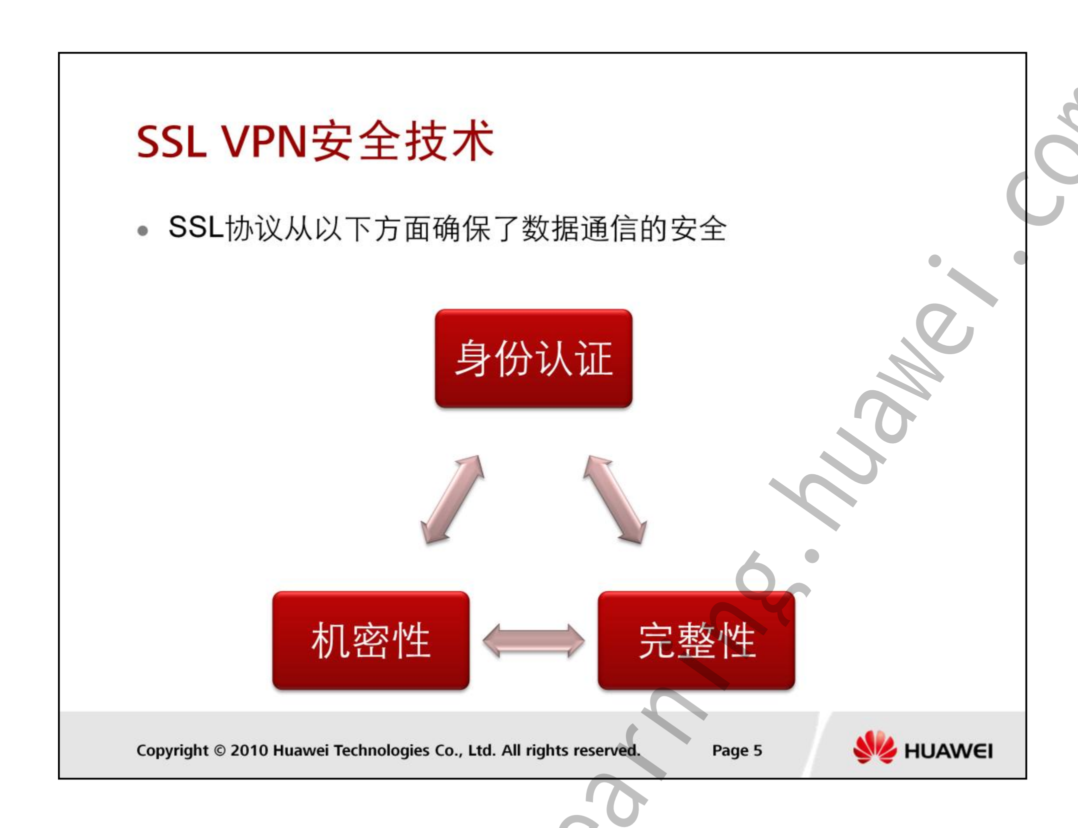
SSL VPN是以SSL/TLS协议为基础，利用标准浏览器都内置支持SSL/TLS的现实优势，对其应用功能进行扩展的新型VPN。除了Web访问、TCP/UDP应用之外，SSL VPN还能够对IP通信进行保护。SSL VPN通信基于标准TCP/UDP，不受NAT限制，能够穿越防火墙，使用户在任何地方都能够通过SSL VPN虚拟网关访问内网资源，使远程安全接入更加灵活简单，大大降低了企业部署维护VPN的费用。

SSL VPN帮助用户使用标准的浏览器，就可以访问企业的内部应用。这使得移动办公人员只要有一台接入了Internet的电脑，就可以随时随地进行安全的远程访问了。SSL VPN的安全性、便捷性和易用性为企业的移动办公带来了便利，使移动员工的工作效率最大化。

要使用SSL协议进行VPN通信，通信双方必须支持SSL。目前常见的应用一般都支持SSL，如IE、Netscape浏览器、Outlook、Eudora邮件应用等。



SSL与IPSec安全协议一样，提供加密和身份验证。但是，SSL协议只对通信双方传输的应用数据进行加密，而不是对从一个主机到另一主机的所有数据进行加密。



SSL协议提供的安全技术：

1. 主体的身份可以通过公钥加密算法来验证。
2. 连接是保密的，在握手协议协商密钥后，用对称密钥加密数据。
3. 连接是可靠的，使用了安全的散列算法，用带密钥的消息认证码来验证消息的完整性

- 身份认证

在建立SSL连接之前，客户端和服务器之间需要进行身份认证，认证采用数字证书，可以是客户端对服务器的认证，也可以是双方进行双向认证。

- 机密性

采用加密算法对需要传输的数据进行加密。

- 完整性

采用数据鉴别算法，验证所接收的数据在传输过程中是否被修改。

传统VPN存在的问题

L2TP及拨号
- 不安全
- 拨号上网的额外费用
- 拨号接入服务器端口限制
- 缺少信息鉴别
- 无基于应用的访问控制策略
- 泄漏内网IP

MPLS
- 不安全
- 无用户认证
- 无应用授权
- 无审计
- 无加密
- 无访问控制
- 造价高
- 跨运营商互通互联问题
- 适用于大型企业内网互联

IPSec
- 客户端管理费用高
- NAT问题
- 安全风险
- 无基于应用的用户认证授权审计

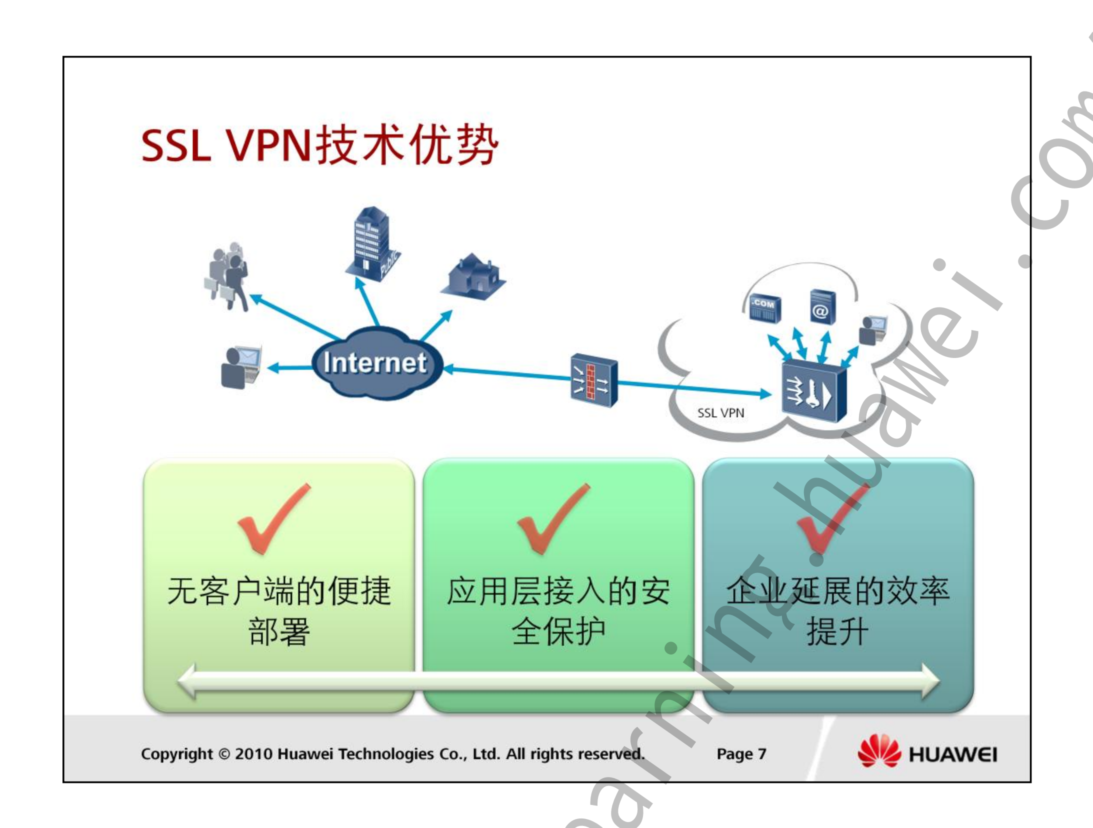
 Page 6 HUAWEI

IPSec VPN可安全、稳定地在两个网络间传输数据，并保证数据的完整无缺，适用于处理总公司与分公司之间的信息往来及其他Site-to-Site应用场景。

由于IPSec是基于网络层的协议，很难穿越NAT和防火墙，特别是在接入一些防护措施较为严格的个人网络和公共计算机时，往往会导致访问受阻。移动用户使用IPSec VPN需要安装专用的客户端软件，为日益增长的用户群发放、安装、配置、维护客户端软件已经使管理员不堪重负。因此，IPSec VPN在Point-to-Site远程移动通信方面并不适用。

SSL VPN 是以SSL/TLS 协议为基础，利用标准浏览器都内置支持SSL/TLS 的现实优势，对其应用功能进行扩展的新型VPN。除了web 访问、TCP/UDP 应用之外，SSLVPN 还能够对IP 通信进行保护。SSL VPN 通信基于标准TCP/UDP，不受NAT 限制，能够穿越防火墙，使用户在任何地方都能够通过SSL VPN 虚拟网关代理访问内网资源，使得远程安全接入更加灵活简单，大大降低了企业部署维护VPN 的费用。

SSL VPN是面向应用的VPN，具有更好的底层无关性。它的易用性、无客户端应用很好满足了远程访问的需要，保证移动用户随时随地建立安全可控的通信连接。



- 无客户端的便捷部署：
  - 无需改变内网网络结构即可实现快速部署
  - 节省投资，技术支持和管理成本
  - 不存在网络地址转换(NAT)穿越问题
- 应用层接入的安全保护：
  - 用户只能通过SSL VPN接入企业应用资源，一定程度遏制了网络病毒的传播
  - 针对具体的应用资源的细粒度访问控制
- 企业延展的效率提升：
  - 任何时间，任何地点，任何设备的灵活安全接入
  - 企业移动/远程员工可以随时随地安全接入企业内网
  - 分支机构安全连接，合作伙伴业务流整合，用户服务远程支持



目录



SSL协议结构

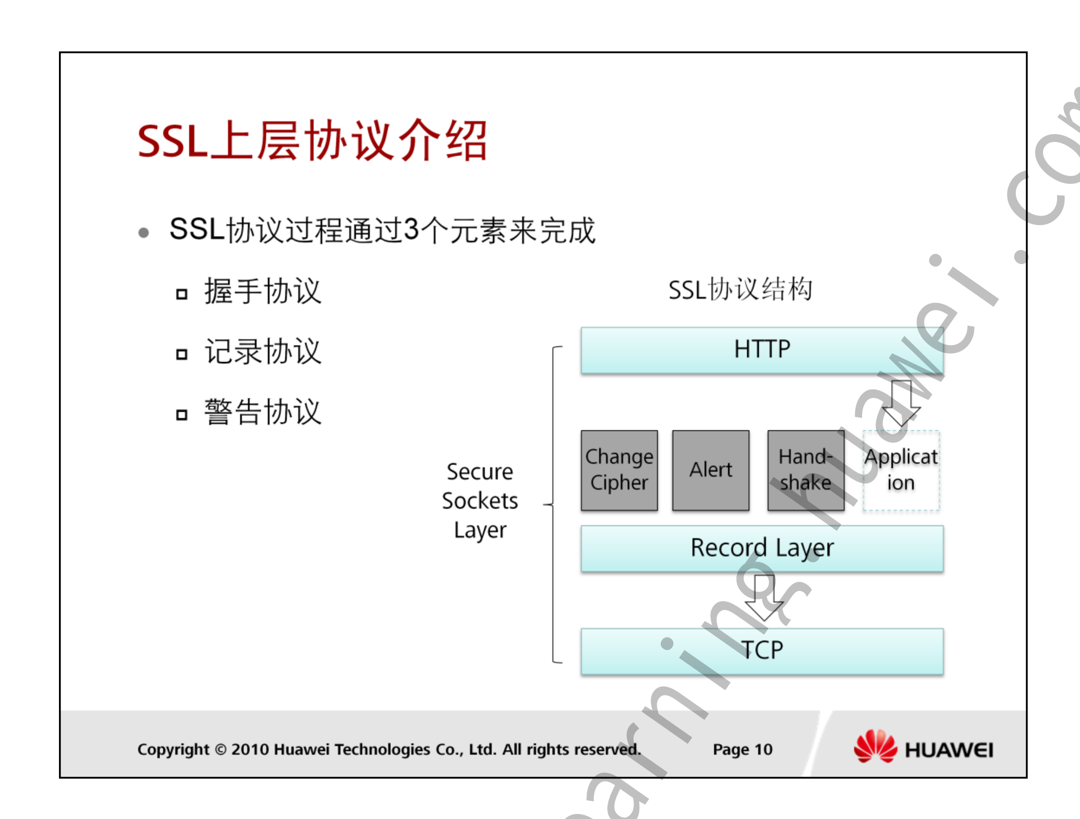
Page 9
HUAWEI

SSL协议结构可以分为两层：

- 底层为SSL记录协议（SSL record protocol）

主要负责对上层的数据进行分块、压缩、计算并添加MAC、加密，最后把记录块传输给对方。

- 上层为SSL握手协议（SSL handshake protocol）、SSL密码变化协议（SSL change cipher spec protocol）和SSL警告协议（SSL alert protocol）
  - SSL握手协议：客户端和服务器通过握手协议建立一个会话。会话包含一组参数，主要有会话ID、对方的证书、加密算法列表（包括密钥交换算法、数据加密算法和MAC算法）、压缩算法以及主密钥。SSL会话可以被多个连接共享，以减少会话协商开销。
  - SSL密码变化协议：客户端和服务器端通过密码变化协议通知接收方，随后的报文都将使用新协商的加密算法列表和密钥进行保护和传输。
  - SSL警告协议：用来允许一方向另一方报告告警信息。消息中包含告警的严重级别和描述。



- 握手协议：

这个协议负责配置用于客户机和服务器之间会话的加密参数。当一个SSL客户机和服务器第一次开始通信时，它们在一个协议版本上达成一致，选择加密算法和认证方式，并使用公钥来生成共享密钥。

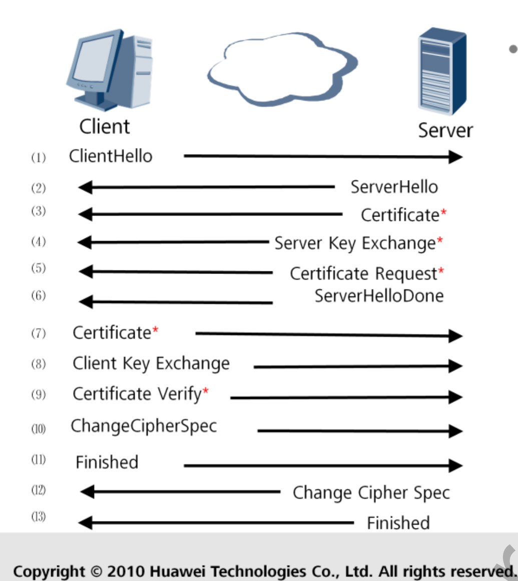
- 记录协议：

这个协议用于交换应用数据。应用程序消息被分割成可管理的数据块，还可以压缩，并产生一个MAC（消息认证代码），然后结果被加密并传输。接收方接收数据并对它解密，校验MAC，解压并重新组合，把结果提供给应用程序协议。

- 警告协议：

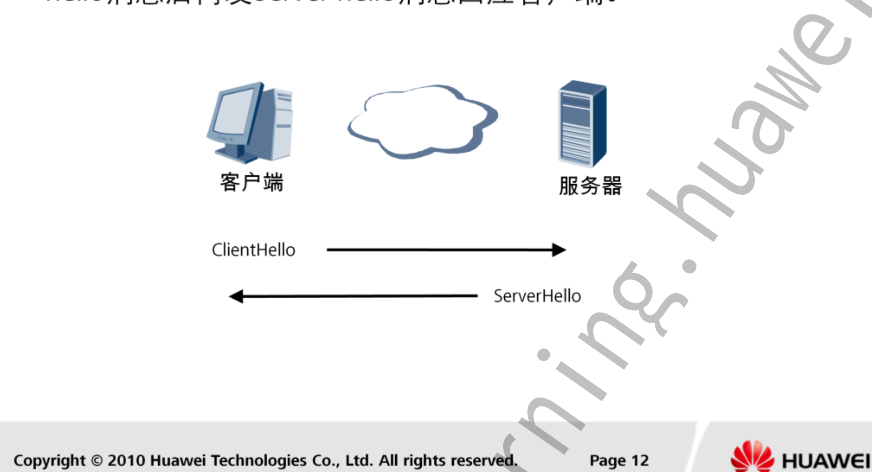
这个协议用于表示在什么时候发生了错误或两个主机之间的会话在什么时候终止。

SSL原理—握手协议



- 在用SSL进行通信之前，首先要使用SSL的HandShake协议在通信两端握手，协商数据传输中要用到的相关安全参数（如加密算法、共享密钥、产生密钥所要的材料等），并对对端的身份进行验证。



- 握手第一阶段：

建立起安全能力属性，客户端发送一个client_hello消息，包括以下参数：

版本：消息中协议版本是两个byte长度分别表示主次版本。目前SSL拥有的版本有SSLv1 SSLv2以及TSLv1（既SSLv3）

随机数：32位时间戳+28字节随机序列,用于在后面计算所有消息的摘要或计算主密钥

会话ID：SSL会话ID标识一次会话用，可以重用。

客户支持的密码算法列表(CipherSuite)：密钥套件列表，列表中包含了Client端支持的所有密钥套件。

客户支持的压缩方法列表：客户端支持的压缩算法列表，填0表示空

当服务器收到包含以上信息的client hello 数据包后，服务器发送server_hello消息，并包括以下参数：

版本：服务器拿出client hello消息中的版本号，再看看自己支持的版本列表，选个两者都支持的最高版本号定为这次协商出来的SSL协议使用的版本。

服务器产生的随机数：此处产生的随机数与client hello消息中的类似。

会话ID：服务端检测到传过来的session ID是空或者检索session 列表没有发现传过来的session id就会新建一个。

服务器从客户建议的密码算法中挑出一套（Ciphersuit ）密码算法。

服务器从客户建议的压缩方法中挑出一个压缩算法。



第二阶段:

- Server certificate消息（可选）

一般情况下，除了会话恢复时不需要发送该消息，在SSL 握手的全流程中，都需要包含该消息。消息包含一个X.509证书，证书中包含公钥，发给客户端用来验证签名或在密钥交换时候给消息加密。

- Server Key Exchange(可选)

根据之前在hello信息中包含的ciphersuit信息，决定了密钥交换方式（例如RSA或者DH），因此在server key exchange消息中便会包含完成密钥交换所需的一系列参数。

- Certificate Request(可选)

服务器端发出client cert request 消息，要求客户端发他自己的证书过来进行验证。该消息中包含server端支持的证书类型(RSA，DSA，ECDSA等。。。)和server端所信任的所有证书发行机构的DN（Distinguished Name）列表，客户端会用这些信息来筛选证书。

- Server Hello Done.

该消息表示server已经将所有信息发送完毕，接下来等待client端的消息。



第三阶段:

- Client certificate(可选):

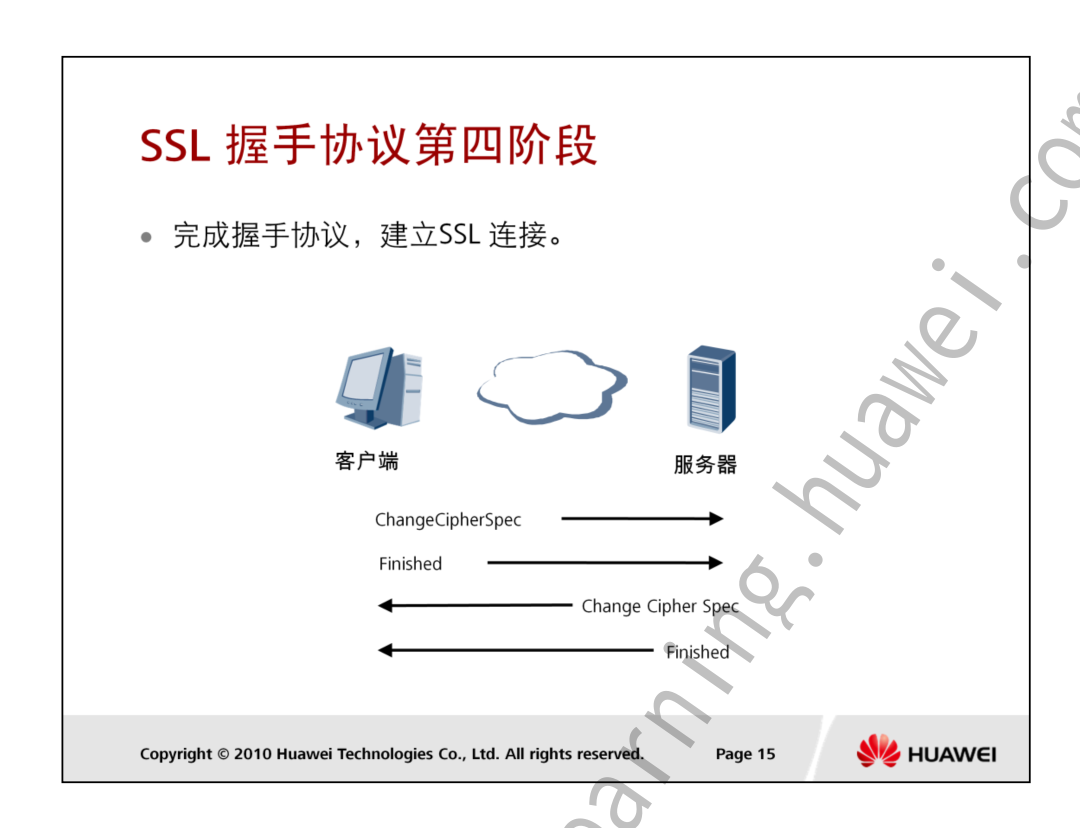
如果在第二阶段server端要求发送客户端证书，客户端便会在该阶段将自己的证书发送过去。Server端在之前发送的certificate request消息中包含了server端所支持的证书类型和CA列表，因此客户端会在自己的证书中选择满足这两个条件的第一个证书发送过去。若客户没有证书，则发送一个no_certificate警告。

- Client Key exchange:

根据之前从server端收到的随机数，按照不同的密钥交换算法，算出一个pre-master，发送给server端，server端收到pre-master算出main master.而客户端当然也能自己通过pre-master算出main master.如此以来双方就算出了对称密钥。

- Certificate verify（可选）:

只有在客户端发送了自己证书到服务器端，这个消息才需要发送。其中包含一个签名，对从第一条消息以来的所有握手消息的HMAC值(用master_secret)进行签名。



第四阶段:

- 建立起一个安全的连接，客户发送一个change_cipher_spec消息，并且把协商得到的CipherSuite拷贝到当前连接的状态之中。然后，客户用新的算法、密钥参数发送一个finished消息，这条消息可以检查密钥交换和认证过程是否已经成功。其中包括一个校验值，对所有以来的消息进行校验。服务器同样发送change_cipher_spec消息和finished消息。握手过程完成，客户和服务器可以交换应用层数据。

SSL原理—会话恢复

Client

Server

(1) ClientHello →

(2) ← ServerHello

(3) ← ChangeCipherSpec

(4) ← Finished

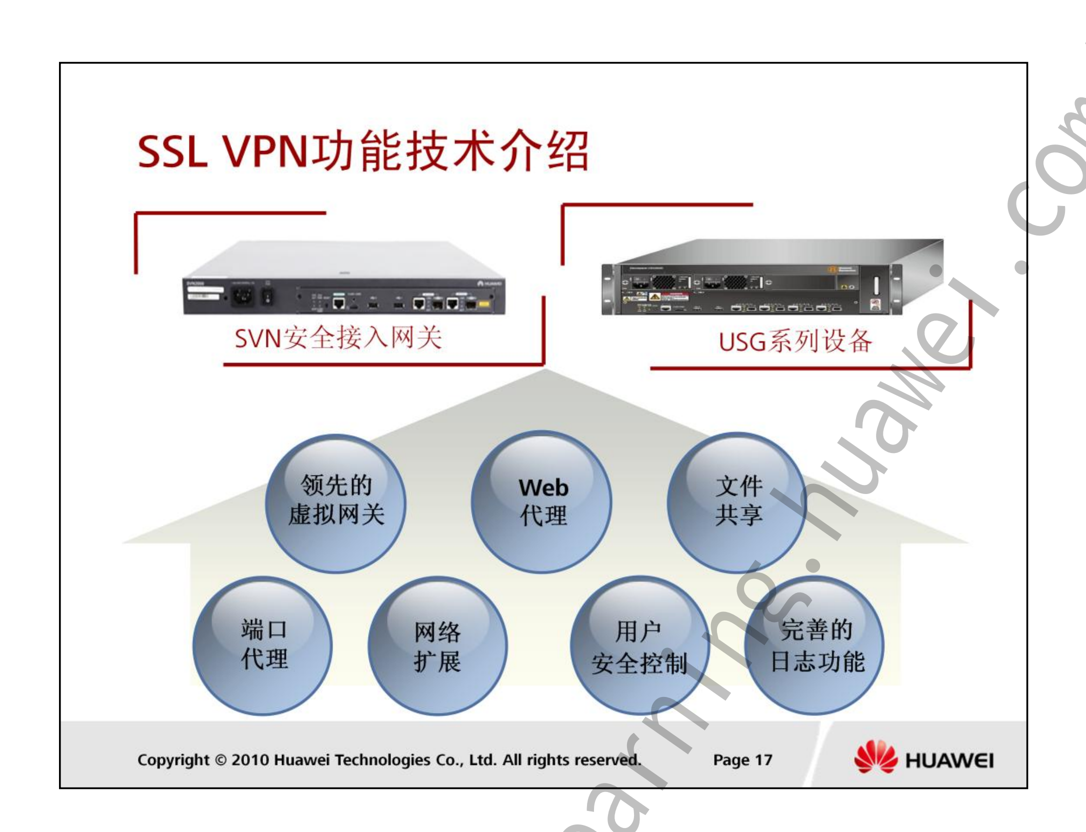
(5) ChangeCipherSpec →

(6) Finished →

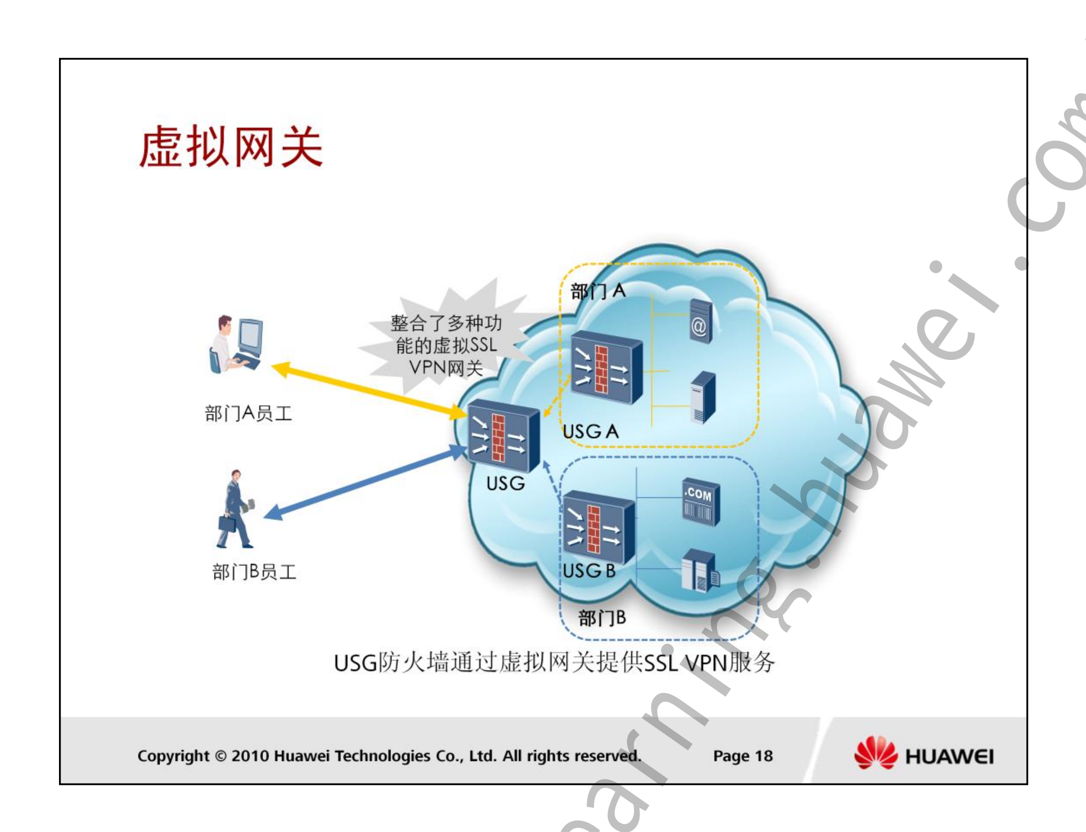
- 会话恢复是指只要客户端和服务器已经通信过一次，它们就可以通过会话恢复的方式来跳过整个握手阶段而直接进行数据传输。
- SSL采用会话恢复的方式来减少SSL握手过程中造成的巨大开销。

 Page 16 HUAWEI

此功能从原来正常协调的13步，减少到只需要7步，大大减少了SSL VPN隧道建立所需要的开销。



- 主要功能包括:
  - 领先的虚拟网关
  - Web代理
  - 文件共享
  - 端口代理
  - 网络扩展
  - 用户安全控制
  - 完善的日志功能



每个虚拟网关都是独立可管理的，可以配置各自的资源、用户、认证方式、访问控制规则以及管理员等；

当企业有多个部门时，可以为每个部门或者用户群体分配不同的虚拟网关，从而形成完全隔离的访问体系。

Web代理

- 实现对内网Web资源的安全访问
  - Web代理实现了无客户端的页面访问
  - Web代理有两种实现方式：Web-link和Web改写

远程用户 Internet USG WEB服务器

 Page 19 HUAWEI

Web代理实现了无客户端的页面访问，充分体现了SSL VPN的易用性，是SSL VPN区别于其他VPN的一个重要功能。它将远端浏览器的页面请求（采用https协议）转发给web服务器，然后将服务器的响应回传给终端用户，提供细致到URL的权限控制，即可控制到用户对某一张具体页面的访问。

Web代理有两种实现方式：Web-link和Web改写；

- Web-link采用ActiveX控件方式，对页面进行转发；
- Web改写方式采用脚本改写方式，将请求所得页面上的链接进行改写，其他网页内容不作修改。

- 使用Web-link方式的优势：
  - 无需安装客户端，只需要标准的浏览器便可远程访问内网web资源。
  - 针对每个URL，为不同的用户分配不同的访问权限。
- 实现过程：
  - 远程接入用户通过SVN网关对企业内网某一web页面发起访问请求
  - 内网服务器将请求结果返回给SVN，由SVN将获取的页面返回给用户
  - 对用户来说，SVN相当于web服务器，而对内部服务器来说，SVN又充当了客户端的角色。

文件共享

- 提供对内网文件系统的安全访问
  - 采用协议转换技术，无需安装专用客户端，直接通过通用浏览器安全接入内部文件系统；
  - 将客户发起的文件共享请求转换成相应的协议格式，与服务器进行交互
  - 支持：
    - SMB协议（Windows）
    - NFS协议（LINUX）

支持Windows(SMB)/UNIX(NFS)文件

新建文件夹

浏览文件

下载文件

上传文件

删除文件(夹)

改名文件(夹)

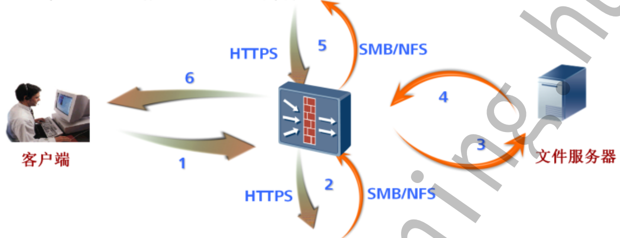
Page 20

HUAWEI

文件共享的主要功能是将不同的系统服务器（如支持SMB协议的Windows系统，支持NFS协议的Linux系统）的共享资源以网页的形式提供给用户访问。

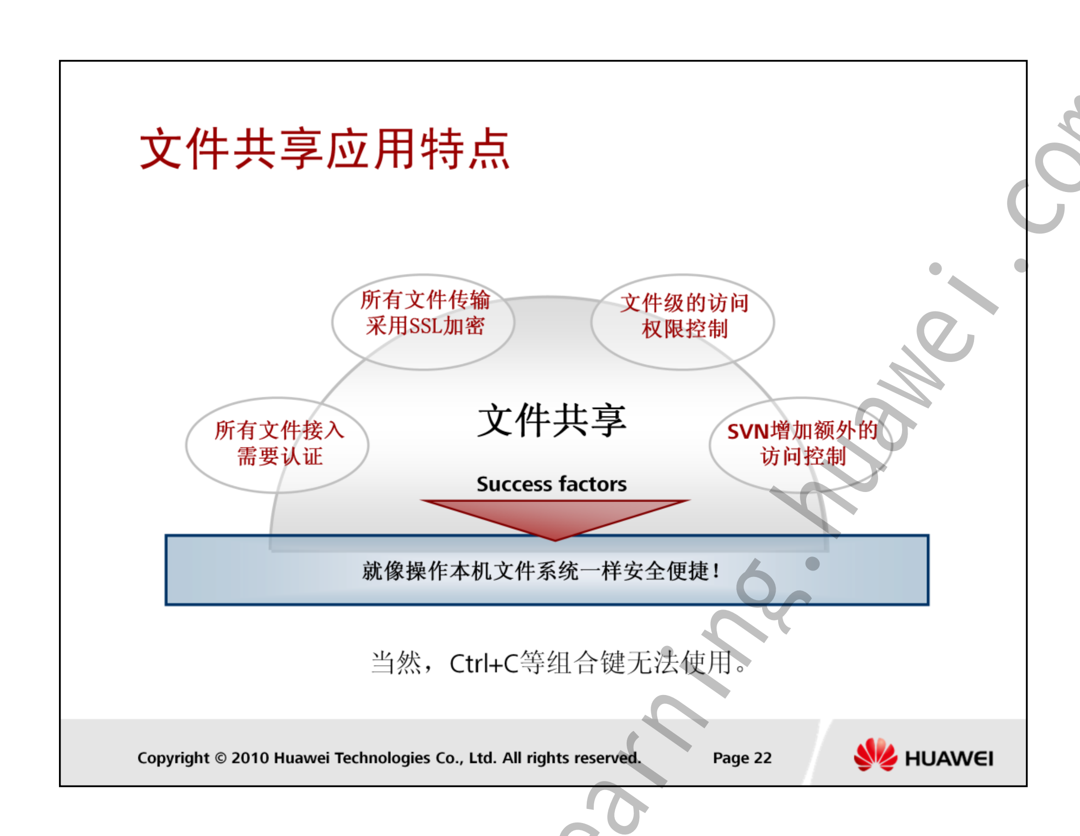
文件共享实现过程

- 以访问内网Windows文件服务器为例：
  - 客户端向内网文件服务器发起HTTPS格式的请求，发送到USG防火墙；
  - USG防火墙将HTTPS格式的请求报文转换为SMB格式的报文；
  - USG防火墙发送SMB格式的请求报文给文件服务器。
  - 文件服务器接受请求报文，将请求结果发送给USG防火墙，用的是SMB报文；
  - USG防火墙将SMB应答报文转换为HTTPS格式；
  - 将请求结果（HTTPS格式）发送到客户端；





 Page 21 HUAWEI



文件共享作为文件服务器的代理，使客户可以安全的访问内网文件服务器。

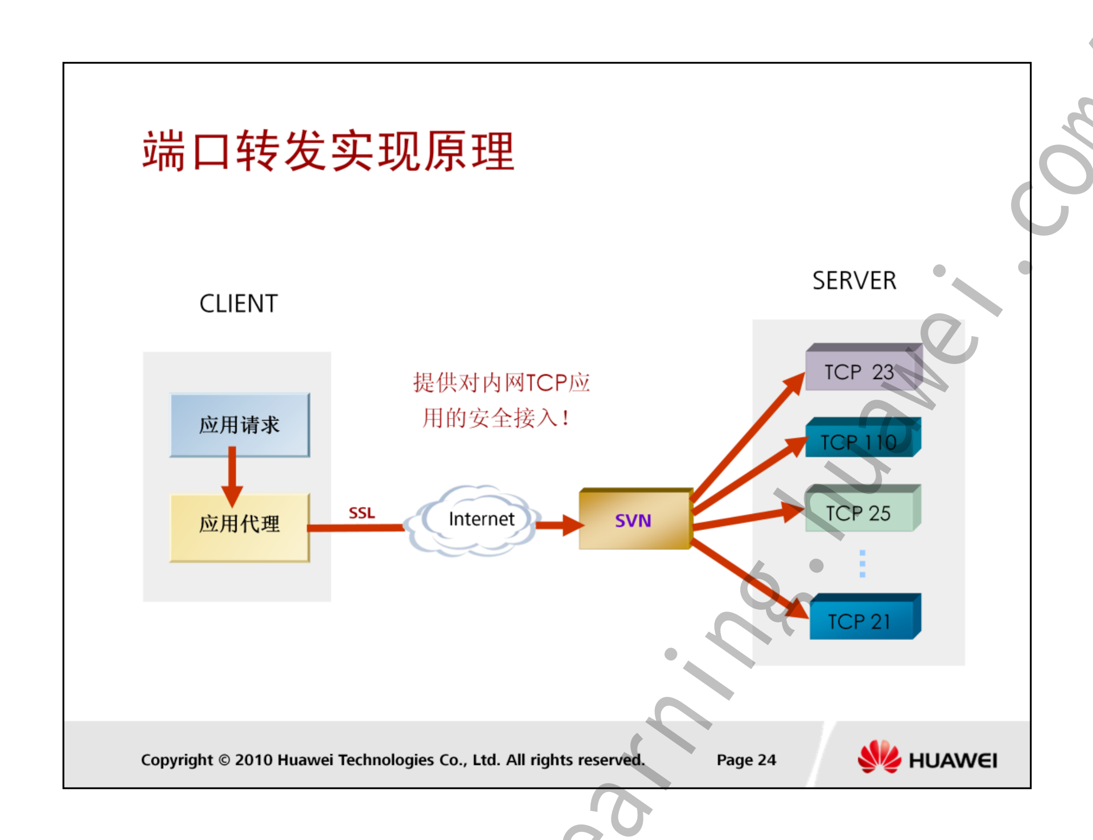
端口转发

- 提供丰富的内网TCP应用服务
  - 广泛支持静态端口的TCP应用
    - 单端口单服务器（如：Telnet，SSH，MS RDP，VNC等）
    - 单端口多服务器（如： Lotus Notes）
    - 多端口多服务器（如： Outlook ）
  - 支持动态端口的TCP应用
    - 动态端口（如： FTP，Oracle）
  - 提供端口级的访问控制

 Page 23 

端口转发功能主要用于C/S等不能使用web技术访问的应用。

- 支持静态端口的TCP应用
  - 单端口单服务：一个服务对应一个端口。 例如：Windows远程桌面、Telnet、SSH（Secure Shell）、VNC、ERP（Enterprise Resource Planning）、SQL（Structured Query Language） Server、iNotes、OWA（Outlook Web Access）、BOSS（Business and Operation Support System）。
  - 单端口多服务：多个服务对应一个端口。 例如：Notes（多个数据库服务器对应一个端口）。
  - 多端口单服务：一个服务对应多个端口。 例如：POP3（Post Office Protocol 3）Email（SMTP（Simple Message Transfer Protocol）：25、POP3：110等）。
- 支持动态端口的TCP应用
  - 动态端口服务：一个服务对应多个动态变化的端口。 例如：FTP被动模式、Oracle Manager。

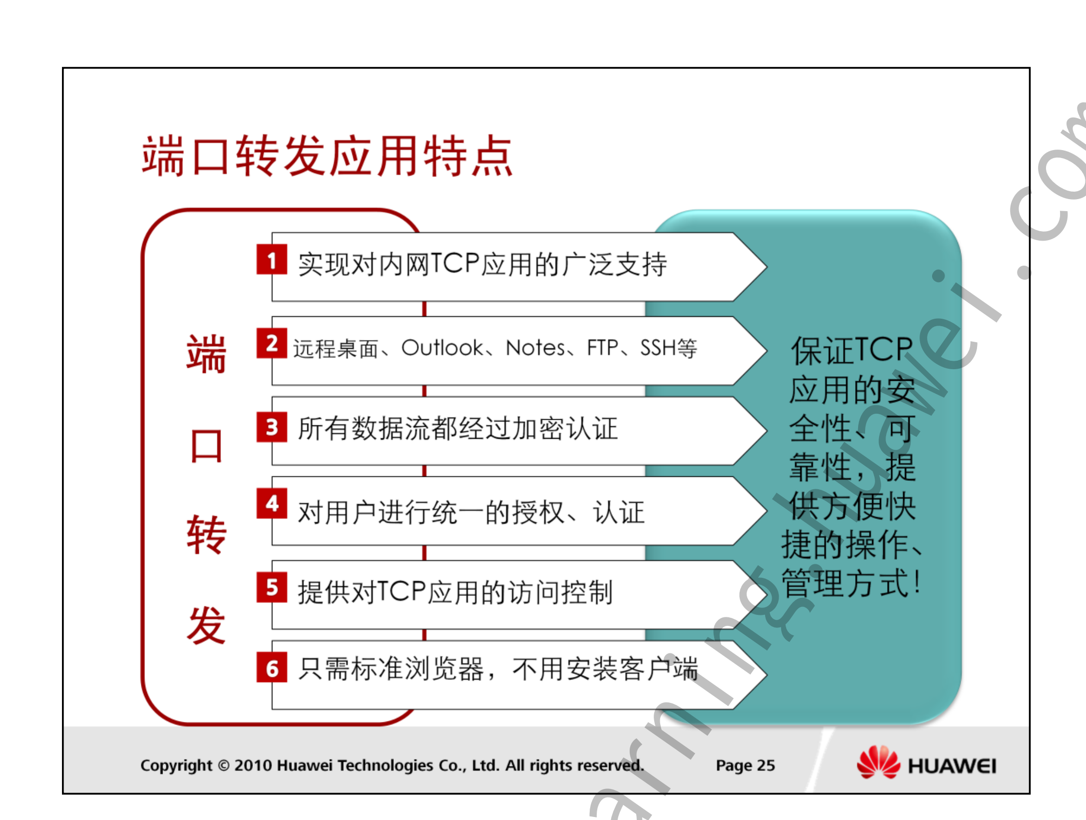


用户点击客户端页面“启动端口转发功能”按钮，自动安装运行一个Windows ActiveX控件，获取到管理端配置的端口转发资源列表（目的服务器IP、端口）。控件将客户端发起的TCP报文与资源列表进行比对，当发现报文的目的IP/Port 与资源列表中的表项匹配，则截获报文，开启侦听端口（目的端口经过特定算法得出），并将目的地址改写为回环地址，转发到侦听端口。

对该报文加密封装，添加私有报文头，将目的地址设为SVN的IP地址，经由侦听端口发往SVN。

SVN收到报文进行解密，发往真实的目的服务器端口。

SVN收到服务器的响应后，再加密封装回传给用户终端的侦听端口。


端口转发应用特点
端
口
转
发
1 实现对内网TCP应用的广泛支持
2 远程桌面、Outlook、Notes、FTP、SSH等
3 所有数据流都经过加密认证
4 对用户进行统一的授权、认证
5 提供对TCP应用的访问控制
6 只需标准浏览器，不用安装客户端
保证TCP应用的安全性、可靠性，提供方便快捷的操作、管理方式！
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 25
HUAWEI

网络扩展

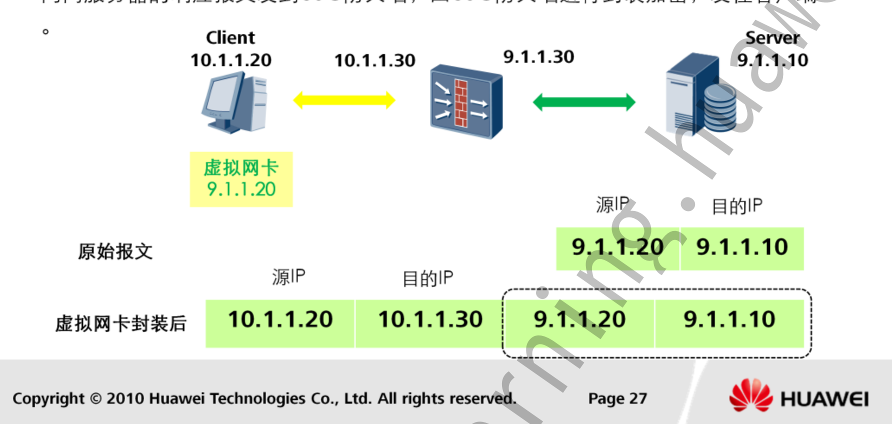
- 实现对内网所有复杂应用的全网访问
  - 通过建立安全SSL隧道，实现对基于IP的内网业务的全面访问
  - 实现方式：
    - ActiveX控件；
    - 专用客户端软件：一次安装，零配置；
  - 访问方式
    - 全路由模式（Full Tunnel）
    - 分离模式（Split Tunnel ）
    - 手动模式（Manual Tunnel ）



使用网络扩展功能后，远程客户端将获得内网IP地址，就像处于内网一样，可以随意访问任意内网资源。同时对其他正常操作不作影响，可以访问Internet和本地子网。

管理员可以根据不同的应用场景配置相应的访问方式：

- 分离模式：用户可以访问远端企业内网（通过虚拟网卡）和本地局域网（通过实际网卡），不能访问Internet。
- 全路由模式：用户只允许访问远端企业内网（通过虚拟网卡），不能访问Internet和本地局域网。
- 手动模式：用户可以访问远端企业内网特定网段的资源（通过虚拟网卡），对其它Internet和本地局域网的访问不受影响（通过实际网卡）。网段冲突时优先访问远端企业内网。



用户使用SSL网络扩展功能前，首先需要在用户本地终端上安装虚拟网卡。虚拟网卡可以通过以下方式安装：

- 本地终端上安装SVN的网络扩展客户端。
- 登录虚拟网关的Web客户端页面，启动网络扩展功能。

启动网络扩展服务后，虚拟网卡会自动向SVN申请一个虚拟IP地址。SVN支持通过以下方式给虚拟网卡分配IP地址：

- DHCP

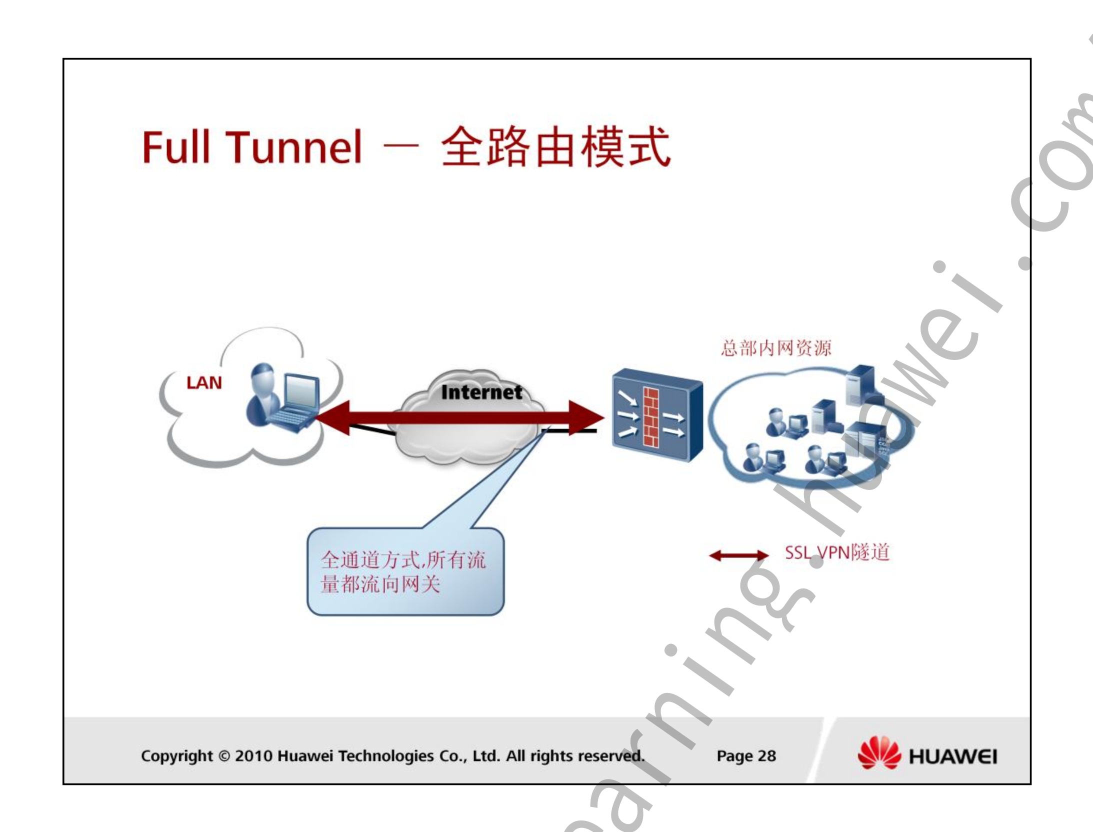
在SVN上配置企业内网的DHCP服务器IP地址。当SVN接收到申请IP地址的请求时，向内网的DHCP服务器请求IP地址，然后分配给客户端。

- 地址池

企业划出一段连续、未使用的IP地址，用作分配给SVN用户的虚拟地址，在SVN上进行配置。IP地址可以随机分配，也可以将用户账号与某一IP地址绑定，则每次该用户启用网络扩展功能时，对用的都是同一内网IP地址。如果绑定的地址包含在地址池内，则该地址就被锁定了，不会分配给另一个用户。

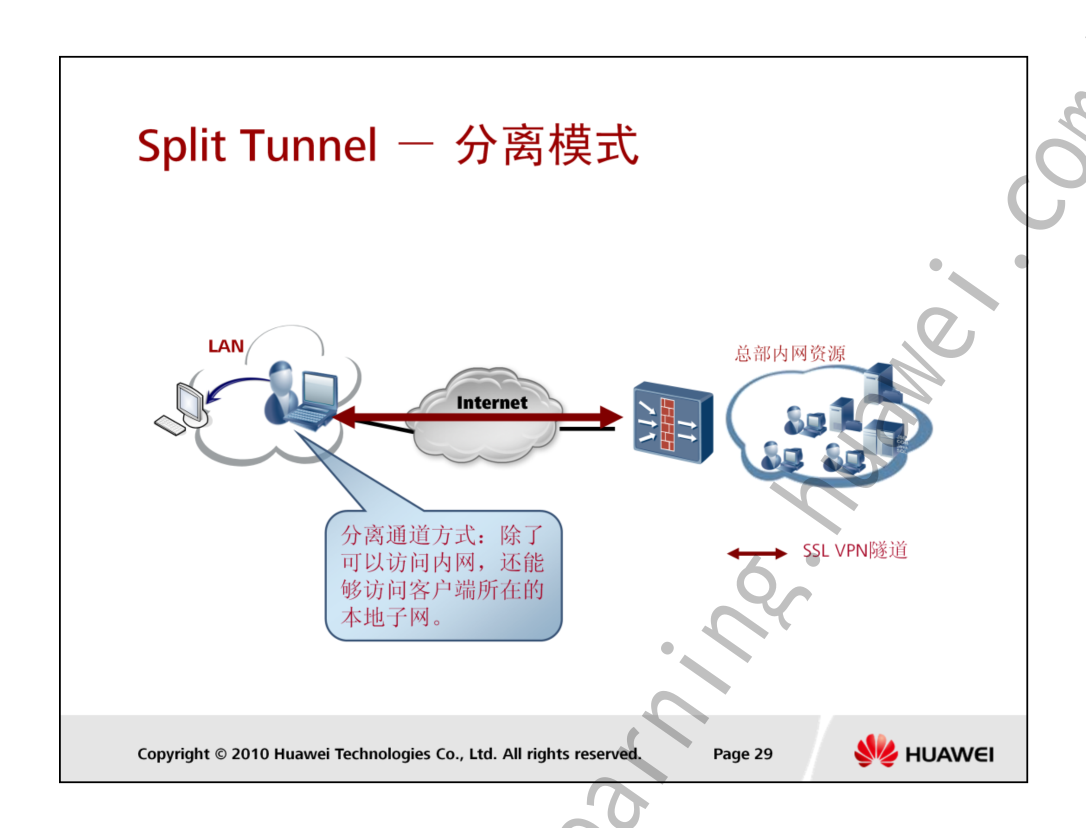
- 外部认证授权服务器

与外部认证授权服务器配合使用，当遇到申请IP地址的请求时，SVN向外部认证授权服务器请求IP地址，然后分配给客户端。

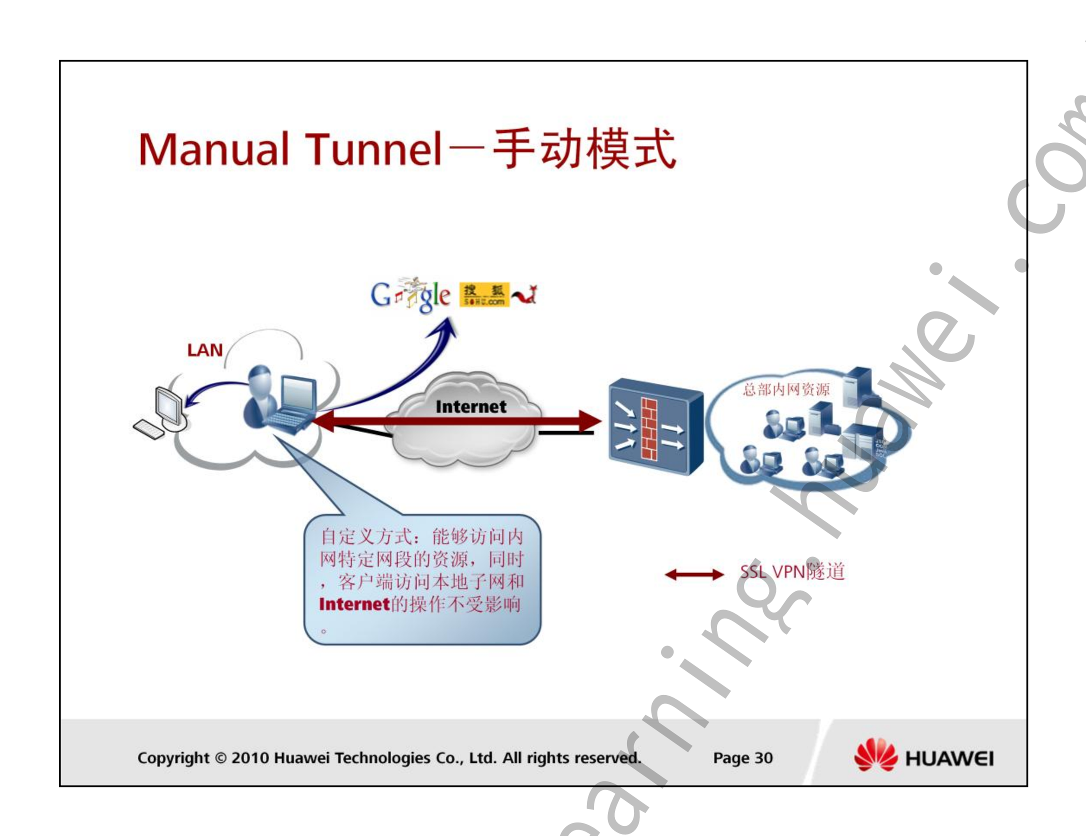


通道模式决定了客户端发送报文的路由。网络扩展功能支持三种通道模式：分离模式、全通道模式、手动模式。

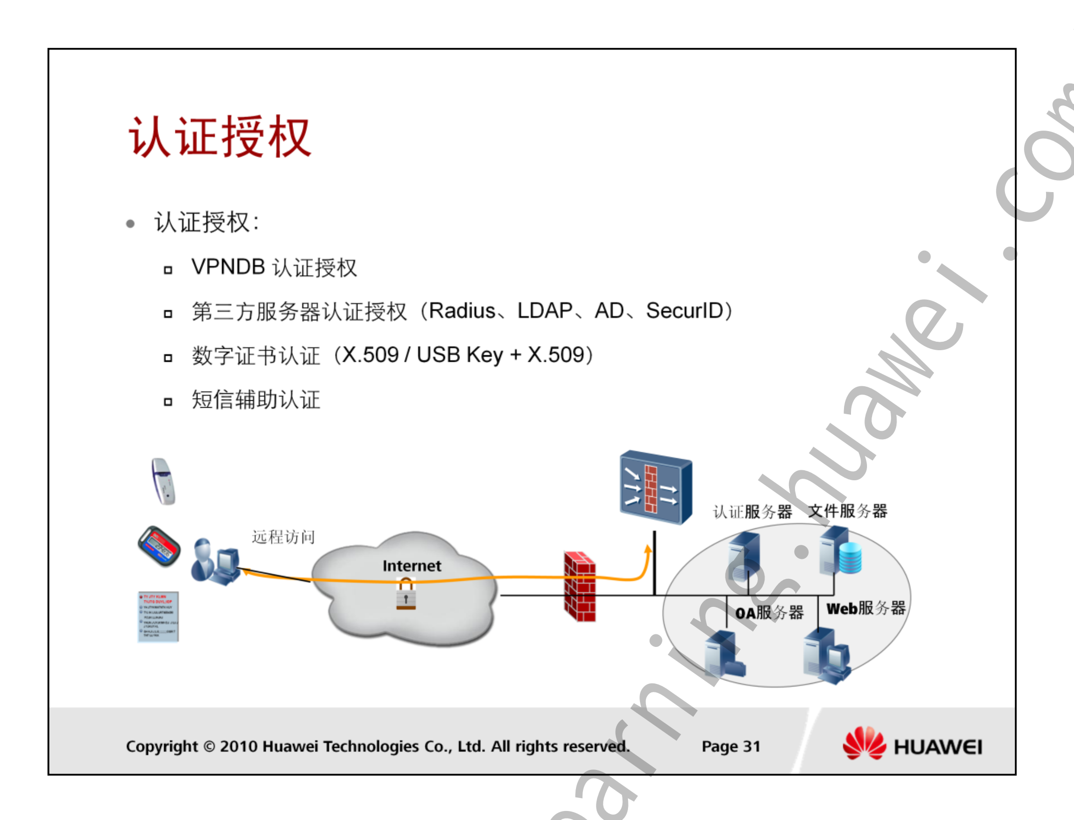
全通道模式：完全屏蔽客户端原先可以访问的网络资源。除了访问远程企业内网资源外，其余网络资源均不可访问。



分离模式： 除了客户端原先可以访问的同一网段的资源，公网等其他资源均被屏蔽。这是因为公网等不同网段资源通过虚拟网卡转发时，由于源IP地址被赋值为虚拟IP地址，所以回复数据往往找不到正确的路由而不能通信成功。



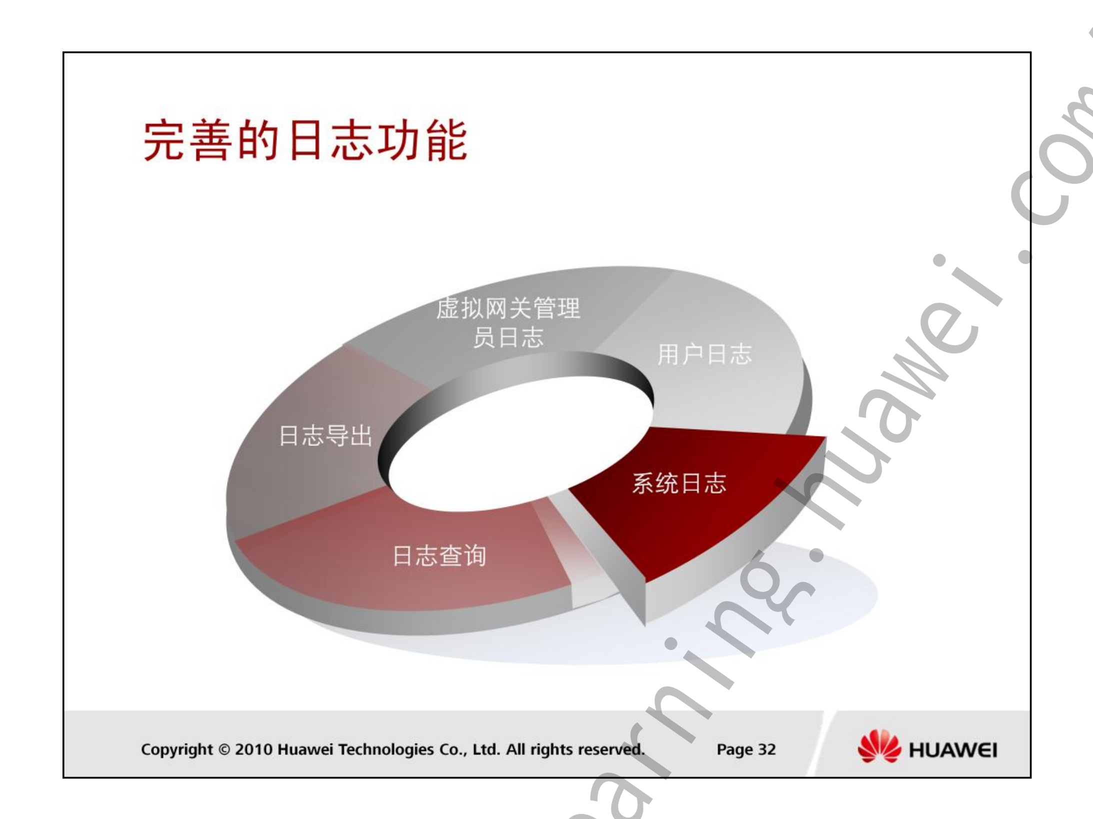
手动模式：除了增加对远程企业内网的访问权限外，不影响客户端原先可访问的网络资源，除非网络资源与远程企业内网冲突。



VPNDB 用于本地VPN 数据库认证与授权，虚拟网关管理员通过用户和组管理来维护VPNDB。本地用户和组管理用于维护VPNDB。分组易于对用户进行管理，可以按组对用户集体授权。

SVN支持通过RADIUS（Remote Authentication Dial In User Service）协议进行远端认证，由网络接入服务器NAS（Network Access Server）作Client 端，与RADIUS 服务器通信。对于RADIUS 协议，可以采用标准RADIUS 协议，与iTELLIN/CAMS 等设备配合完成认证。

SVN支持通过LDAP（Lightweight Directory Access Protocol）协议进行远端认证。



- 系统日志

  系统重启记录，网口状态记录，温度告警记录，导入导出记录，系统管理员管理，虚拟网关管理等；

- 用户日志

  用户登录成功、失败记录，登陆后下线记录，用户修改密码，业务日志；

- 虚拟网关管理员日志

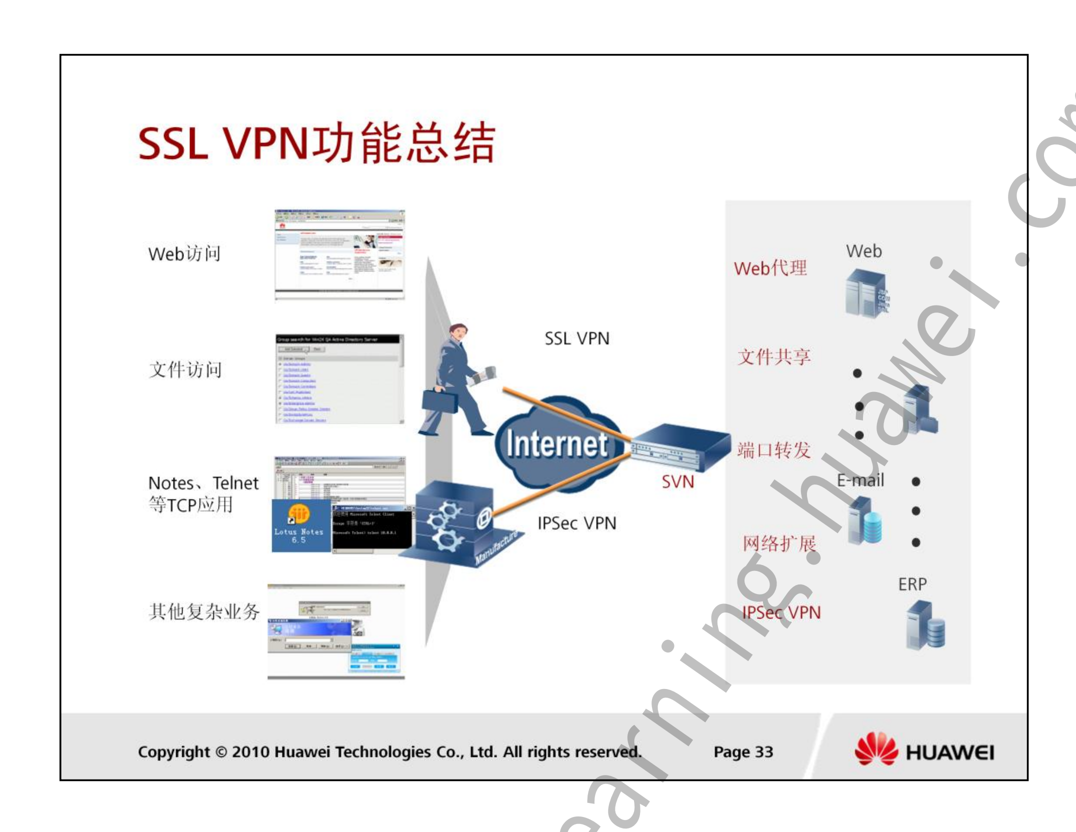
  管理员上线、下线记录，管理员登录失败记录，虚拟网关配置保存，用户管理，安全管理等；

- 日志导出

  日志的实时导出，文本格式的日志导出，命令行日志文件导出等；

- 日志查询

  Web页面日志分级查询，命令行日志查询。



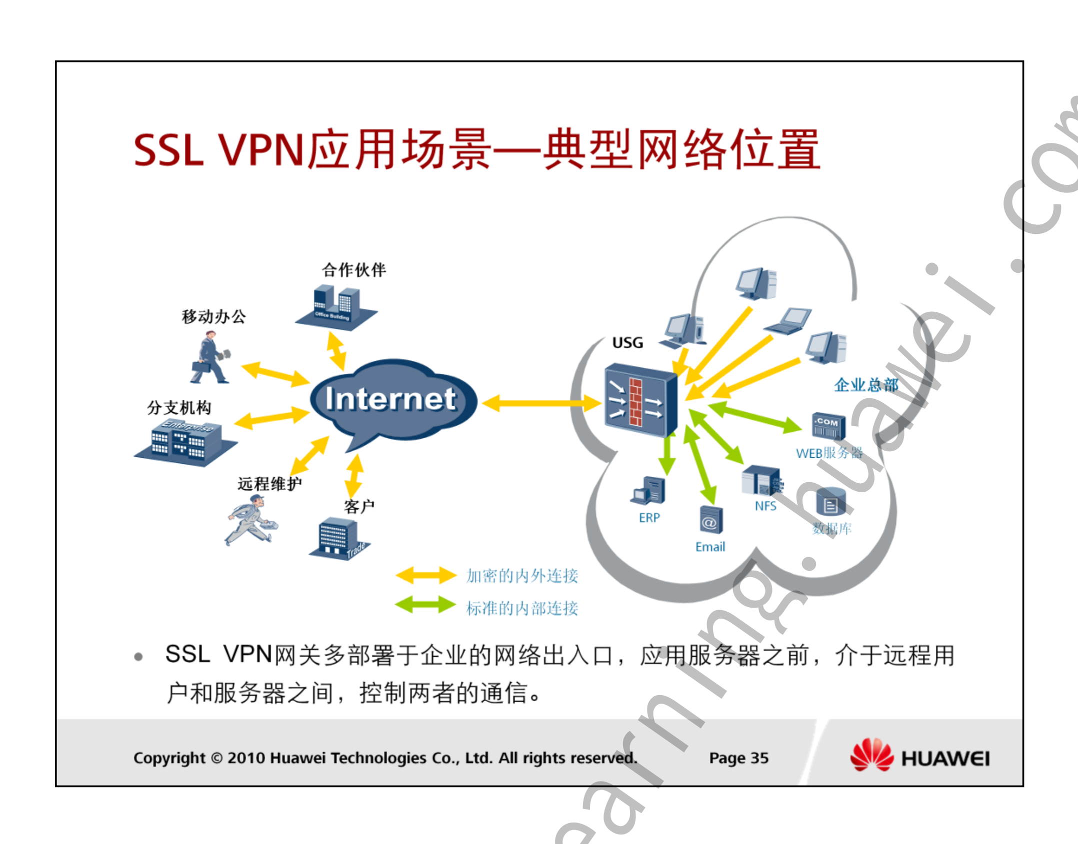
SVN功能总结：

- Web代理
- 文件共享
- 端口转发
- 网络扩展
- IPSec隧道
- 多种认证方式
- 虚拟网关技术
- 细粒度访问控制
- 丰富路由特性(RIP/OSPF)
- VLAN组网
- 双机热备
- 双电源供电
- 完善的日志、审计功能
- ……



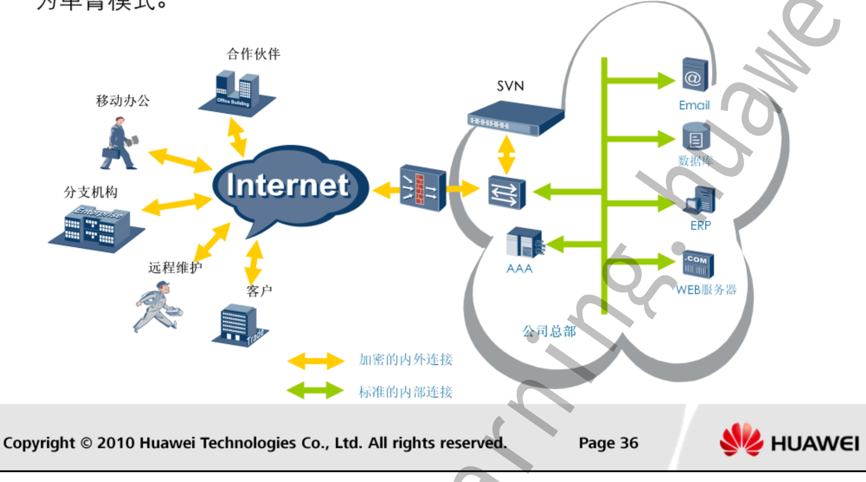
目录





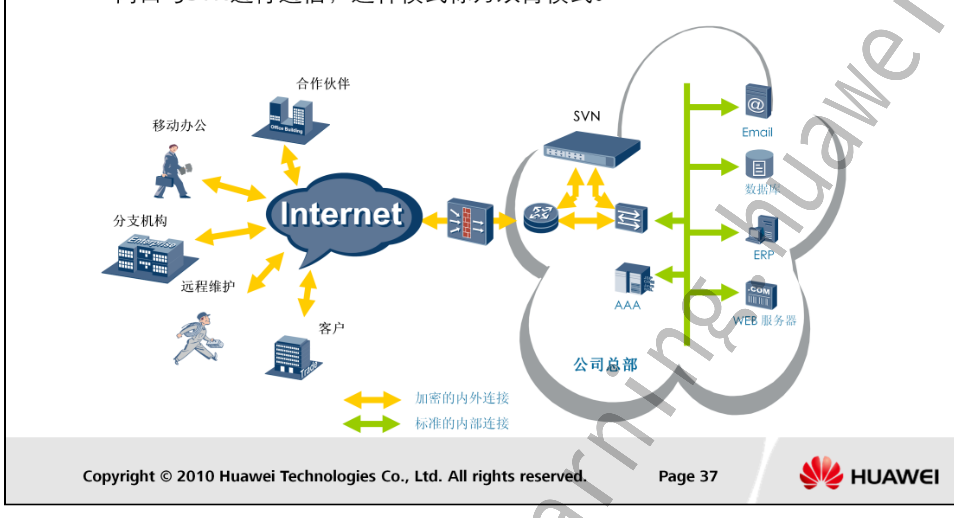
从远程用户到服务器之间的链路分为两段，从SSL VPN网关（如USG防火墙）到服务器之间的数据通信被认为是企业网内部的、安全的，采用标准的TCP/IP协议进行数据通信；而在用户到SSL VPN网关之间的链路，数据在公网上传输，受到各种安全风险的威胁，因此需要对数据进行SSL加密，以防止数据遭到非法的窃听和篡改，保证传输数据的安全性和完整性。

使用该部署方案，在企业出入口放置SSL VPN 安全接入网关（如USG防火墙）实现身份认证和安全通讯。网关可以采用多种认证方式和基于URL的访问控制，帮助用户安全便捷接入企业网络及安全使用内网资源。用户端浏览器与华为 SSL VPN网关之间实现SSL安全通道，确保远程接入访问的安全。



在此类组网环境中，SVN可以直接挂接到企业网络出入口防火墙上，也可以挂接到路由器或者交换机上外网和内网的数据报文从一个网口进出，组网时只用到SVN的一个接口。

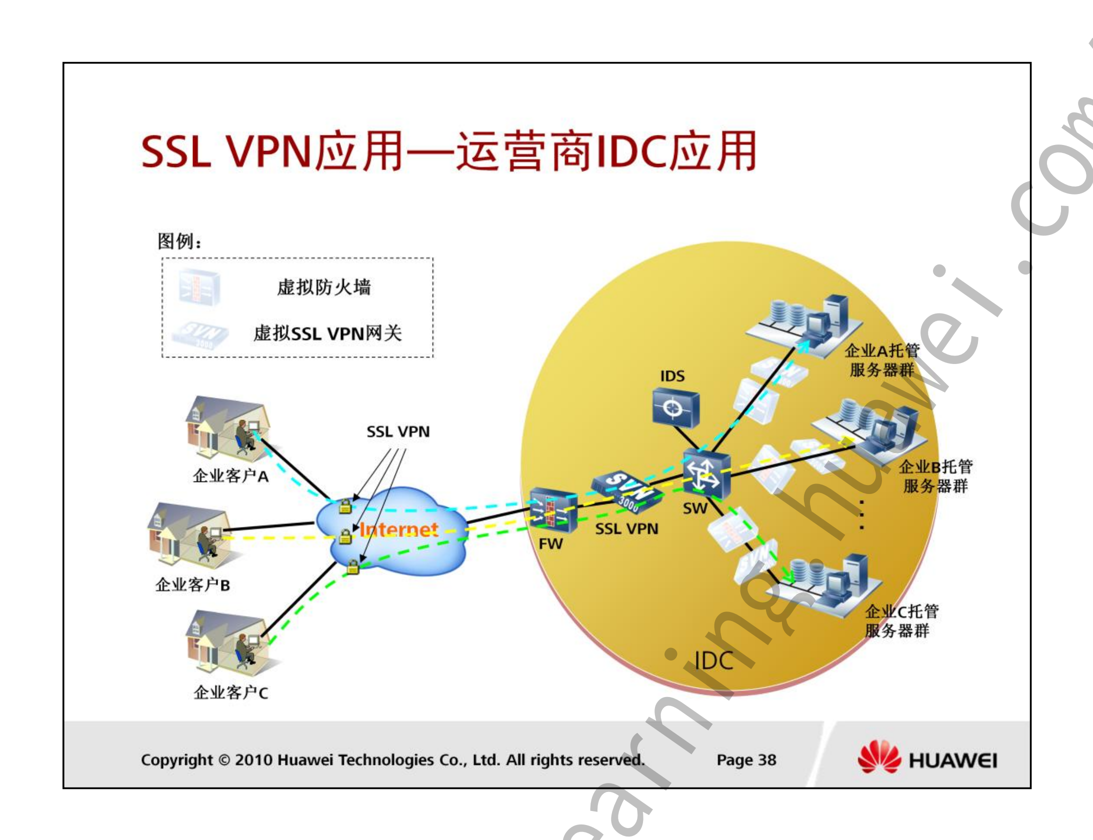
在网络规划时，SVN的接口IP为内网IP地址，此地址需要能与所有被访问需求的服务器路由可达。防火墙上需配置nat server，将SVN的地址映射到防火墙的某一公网IP上。也可以只映射部分端口，如443。如果外网用户有管理SVN的需求，还需要映射SSH、Telnet等端口。



在此类组网环境中，SNV使用两个不同的网口连接外网与内网，这种组网方式下，具有清晰的内网、外网概念；无需做额外的配置，外网口对应虚拟网关IP，内网口配置内网管理IP。

虚拟网关IP不一定需要过NAT转换，只要外网用户能够访问此虚拟网关IP地址即可。内外网接口没有特定的物理接口，任何一个物理接口都可以作为内网或外网接口。

图中路由器和交换机之间处于连接状态。这是因为客户网络中可能有部分应用不需要经过SSL加密，而是直接通过防火墙访问外网。这时就需要在交换机和路由器上配置策略路由，需要建立SSL VPN的流量就转发到SVN上，而普通的应用就直接通过防火墙访问外网。



以上应用为SSL VPN的运营模式。通过把SSL VPN设备划分为数个虚拟设备，每个虚拟设备有自己的管理员及访问策略，依次来降低运营商的资金投入，做到设备使用率最大化。



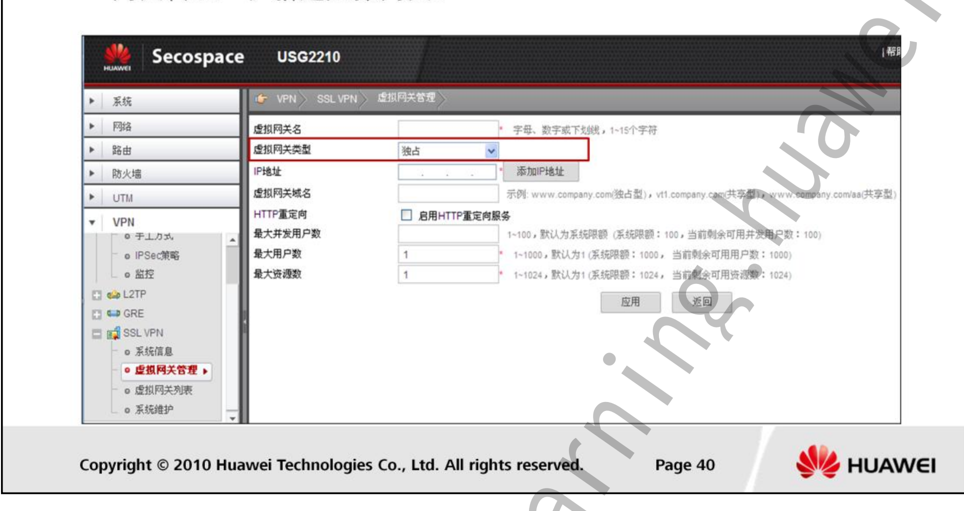
如果绑定Web网管和IP地址时设置的端口号为443以外的端口号，那么在下次登录Web网管输入IP地址时，请在IP地址后面加上“:端口号”，如“https://x.x.x.x:port”，否则将不能登录Web网管。

如果虚拟网关使用的IP地址与Web网管相同，则需要更改Web网管所使用的端口，否则无法完成虚拟网管的配置。

SVN的初始用户名、密码为：admin、Admin@123。

虚拟网关配置及相关参数

- 登录到USG防火墙的Web管理页面后，选择“VPN > SSL VPN > 虚拟网关管理”，新建虚拟网关。



在USG防火墙上配置SSL VPN需要申请购买相应的license。在系统>维护>License管理中可查看到license状态。

虚拟网关按照IP地址和域名的分配情况分为两种:

- 独占型

独占型虚拟网关独占IP地址和域名。客户可以通过域名或者IP地址访问独占型虚拟网关。

- 共享型

多个共享型虚拟网关共享同一个IP地址，具有相同的父域名，通过子域名来区分各虚拟网关。客户只能通过域名访问共享型虚拟网关。

最大并发用户数：同时接入虚拟网关的用户数。

最大用户数：VPNDB

Web代理访问实例（一）

- 在“虚拟网关列表”导航树上单击“Web代理”，进入配置页面。



如果USG上配置了DNS服务器（下面的教材中会介绍），URL处可配置网址，不必一定是IP。

在配置Web代理的基本功能之前，需要准备以下数据：

1. Web资源的名称。
2. Web资源的URL地址。
3. Web资源的描述信息。



使用远程客户端通过SSL VPN隧道登录到USG SSL VPN上，会出现以上页面。在点击链接前，需要先确认Web服务器可达并已配置完成。通过SSL VPN建立的SSL VPN隧道，远程客户端就像在本地内网一下访问内网Web资源。



如果配置了DNS服务器（下面的教材中会介绍），URL处可配置网址，不必一定是IP。

“类型”分为SMB和NFS两种，SMB对应Windows主机，NFS对应Linux主机。

在配置文件共享的基本功能之前，需要准备以下数据：

1. 文件共享资源的名称。
2. 文件共享资源的路径。
3. 文件共享资源的类型。
4. 文件共享资源的描述信息（可选）。



登录到SSL VPN网关上后，会出现以上页面。在点击链接前，需要先确认文件服务器可达并已配置完成。

这里输入的用户名密码与我们平时访问同一局域网内某一共享主机时输入的用户名密码一样。如果不想输入用户名密码，可以在文件共享服务器上设置权限。

文件共享应用举例（三）

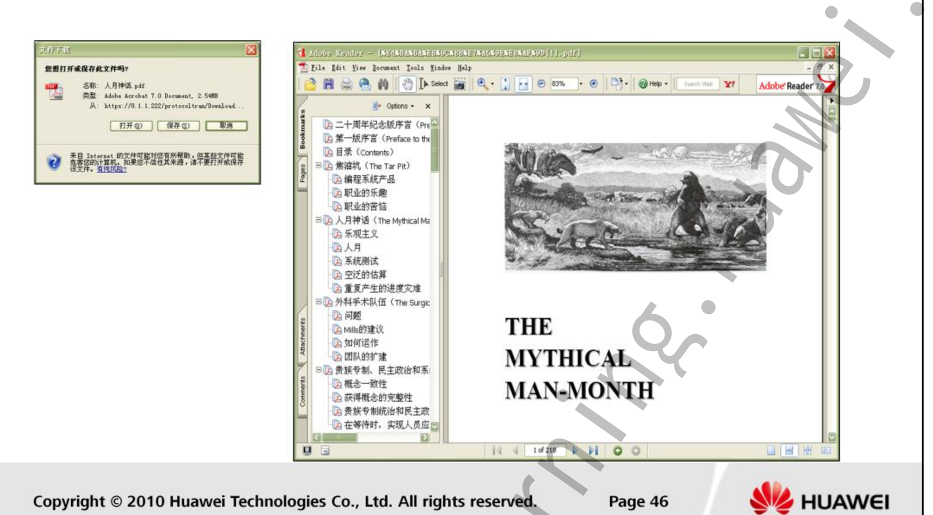
- 看到该共享文件夹下的资源列表：





文件共享应用举例（四）

- 浏览文件：



HUAWEI

端口转发

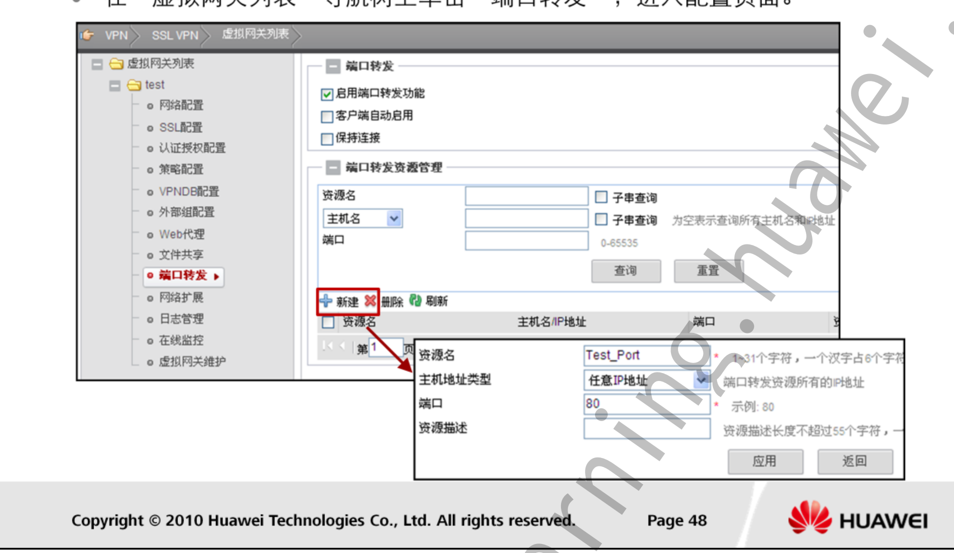
- 提供丰富的内网TCP应用服务
  - 广泛支持静态端口的TCP应用
    - 单端口单服务器（如：Telnet，SSH，MS RDP，VNC等）
    - 单端口多服务器（如： Lotus Notes）
    - 多端口多服务器（如： Outlook ）
  - 支持动态端口的TCP应用
    - 动态端口（如：FTP被动模式，Oracle）
  - 提供端口级的访问控制



 Page 47



端口转发业务是提供基于TCP的应用程序的安全接入，是一种非Web的应用方式。如：Telnet、远程桌面、FTP、Email等服务。



“主机地址类型”分为三类：

- 主机名：填写主机名，需要DNS上有相应配置
- 主机IP地址：填写IP地址
- 任意IP地址：直接填写端口号即可。

端口转发在应用级对用户访问进行控制，可控制是否提供各种应用服务（如：Telnet、远程桌面、FTP、Email等基于TCP连接的服务）。



登录到SSL VPN网关上后，会出现以上页面。在配置端口转发的基本功能之前，需要准备以下数据：

1.端口转发资源的名称。

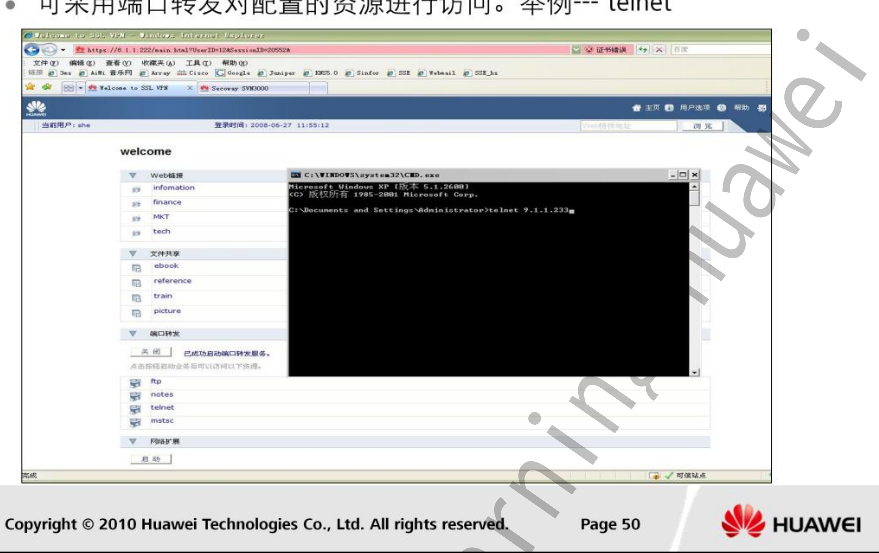
2.端口转发资源的主机名/IP 地址。

3.端口转发资源提供服务的端口。

4.端口转发资源的描述信息（可选）。

端口转发访问实例（三）

- 可采用端口转发对配置的资源进行访问。举例--- telnet



 Page 50 HUAWEI

telnet命令后输入内网实际要访问的设备的IP地址，而不是防火墙或SVN的外网或内网地址。



- DHCP分配方式

为企业已有的DHCP服务器提供接口，通过DHCP来为登录SSL VPN的远端用户分配内网IP地址。

IP地址池是企业划出一段连续、未使用的IP地址，用作分配给SSL VPN用户的虚拟地址。

IP地址可以随机分配，也可以将用户账号与某一IP地址绑定，则每次该用户启用网络扩展功能时，对用的都是同一内网IP地址。

如果绑定的地址包含在地址池内，则该地址就被锁定了，不会分配给另一个用户。

网络扩展访问实例（二）

- 点击网络扩展启动按钮，启动网络扩展功能。



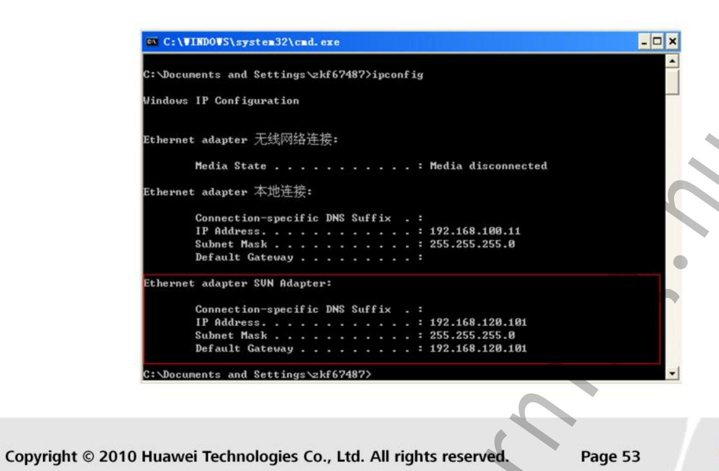
- 网络扩展启动成功后，在电脑任务栏上会提示网络扩展已启动。





网络扩展访问实例（三）

- 查看PC 机的IP地址，已经分配到了地址池中的地址。此时，可以开始使用网络扩展功能访问网络资源。



 Page 53 HUAWEI

此时查看远程客户端的IP地址，可以看到两个网卡。一个为真实网卡，一个为虚拟网卡。

网络扩展访问实例（四）

应用实例—— FTP：

应用实例——登录远程桌面，浏览内网视频文件





VPNDB应用实例（一）

- 在虚拟网管列表中，点击“VPNDB配置”进入此页面。



VPNDB中的用户信息可以单个创建，也可以通过导入文件批量创建。导入的文件类型为“*.txt”。文件中每一行作为一个用户的信息，内容格式为“用户名 密码”或“用户名 密码 UID GID”，每一行以回车换行结束。

在本页面中可配置远程客户端与SSL VPN网关建立SSL VPN隧道所使用的账号，并且可以将此账号加入某个用户组中。

如果配置虚拟IP地址，则将此IP地址和用户名进行了绑定。



总结

- SSL VPN的技术原理
- SVN产品的基本功能和特性
- SSL VPN配置方法



思考题

- SSL VPN主要应用在哪些场景?
- SSL VPN主要可提供哪些安全服务?
- SSL VPN中虚拟网关的作用是什么?
- 独占型、共享型虚拟网关有什么区别？它们之间应用场景各是什么?
- Web代理、文件共享、端口转发和网络扩展的应用场景各是什么?
- 网络扩展有哪3种访问方式？它们之间的实现机制有什么不同?

 Page 57

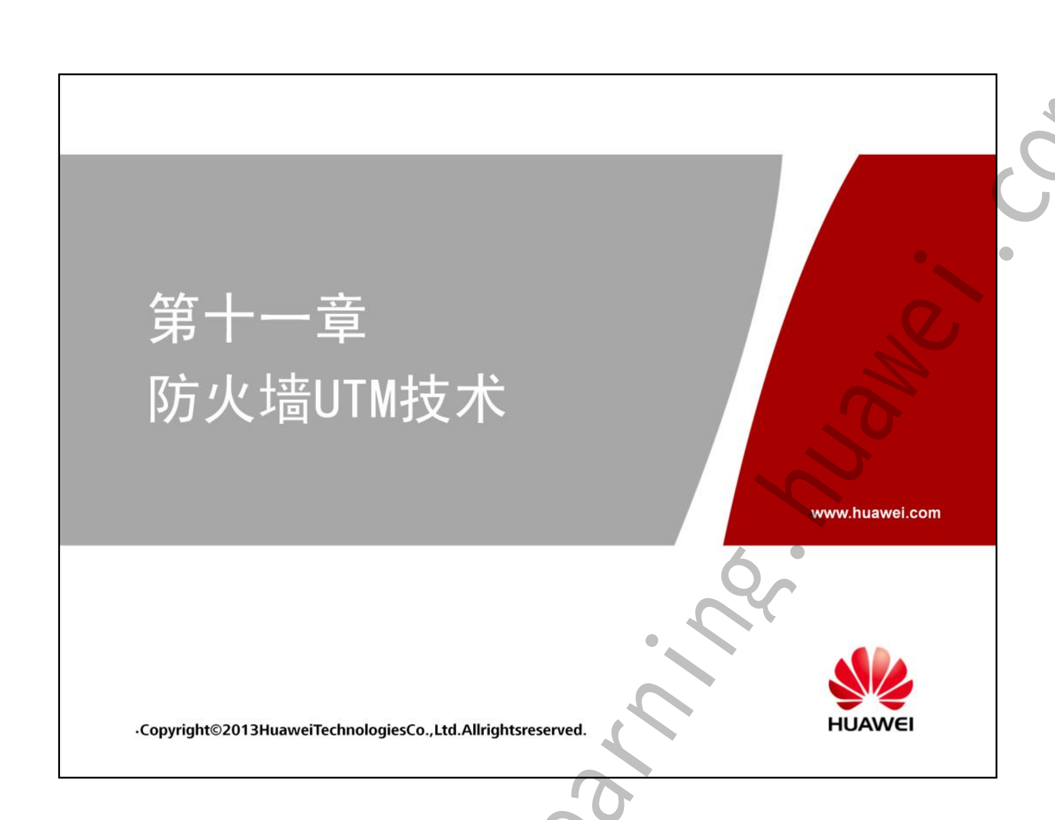


说明：Web代理、文件共享无需使用控件，而端口转发和网络扩展需要控件。

Thank you

www.huawei.com

HC110310011 HCNP-Security-CBSN 第十一章 防火墙 UTM 技术


第十一章
防火墙UTM技术
www.huawei.com
·Copyright©2013HuaweiTechnologiesCo.,Ltd.Allrightsreserved.
HUAWEI



目标

- 学完本课程后，您将能够:
  - 了解防火墙UTM技术产生的背景；
  - 理解防火墙UTM特性；
  - 掌握防火墙UTM特性配置。





目录



网络安全威胁分析

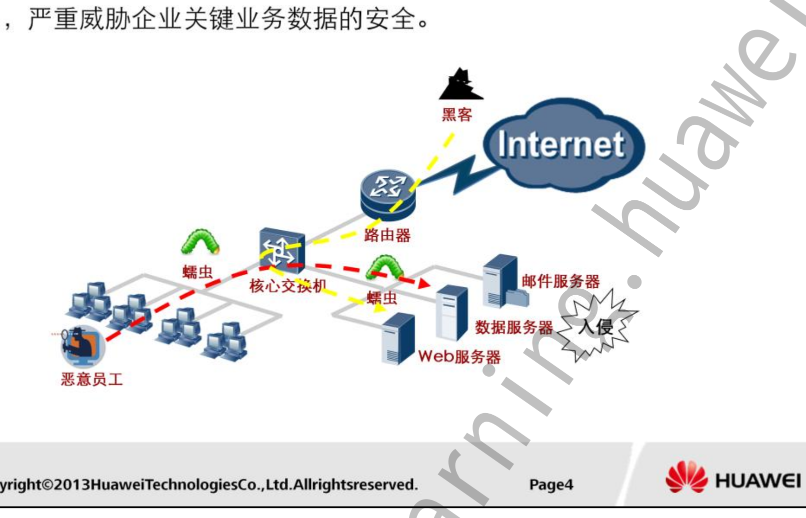
- 网络威胁
  - 黑客入侵、拒绝服务攻击、病毒及恶意软件、个人安全意识薄弱
- 网络威胁的现状
  - 现在大多数病毒等网络威胁不再单纯地攻击电脑系统，而是被黑客攻击和不法分子利用，成为他们获取利益的工具。因此，传统的电脑病毒等网络威胁，正在向由利益驱动的、全面的网络威胁发展变化。

 Page3

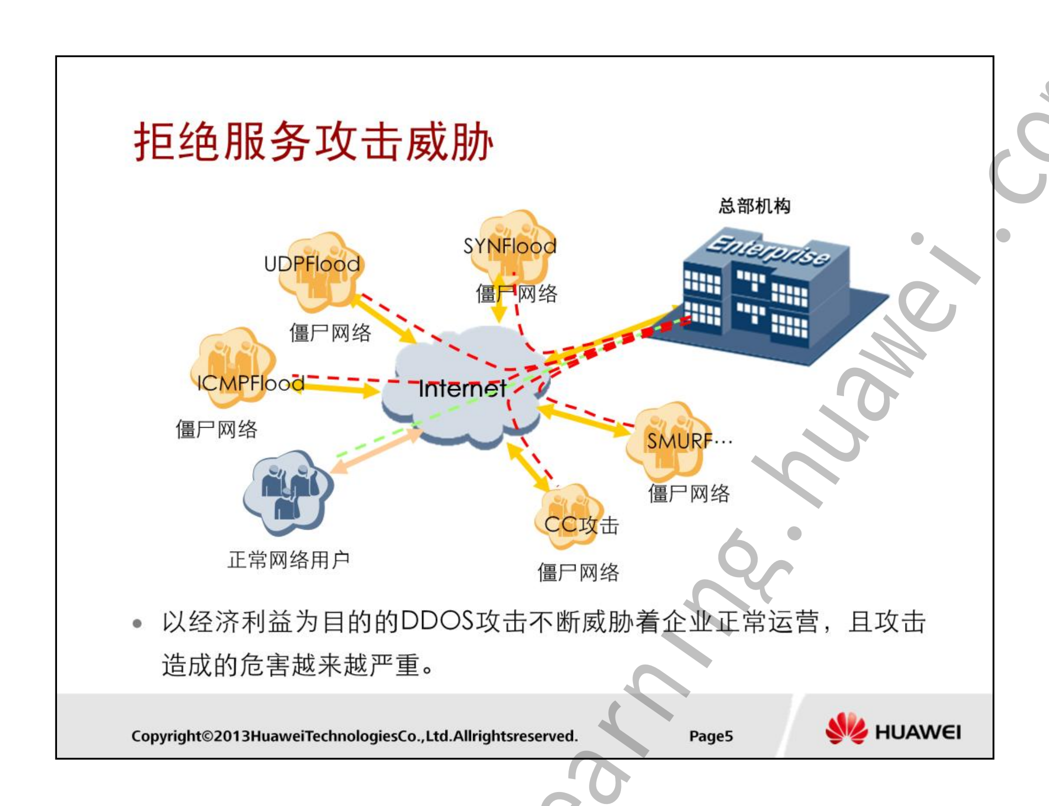


在目前出现的各种安全威胁当中，恶意程序（病毒与蠕虫、Bot、Rootkit、特洛依木马与后门程序、弱点攻击程序以及行动装置恶意程序）类别占有很高的比例，灰色软件（间谍/广告软件）的影响也逐渐扩大，而与犯罪程序有关的安全威胁已经成为威胁网络安全的重要因素。

目前用户面临的不再是传统的病毒攻击，“网络威胁”经常是融合了病毒、黑客攻击、木马、僵尸、间谍等危害等于一身的混合体，因此单靠以往的防毒或者防黑技术往往难以抵御。



- 服务器漏洞给企业造成严重的安全威胁：
- 企业内网中许多应用软件可能存在漏洞；
- 互联网使应用软件的漏洞迅速传播；
- 蠕虫利用应用软件漏洞大肆传播，消耗网络带宽，破坏重要数据；
- 黑客、恶意员工利用漏洞攻击或入侵企业服务器，业务机密被篡改、破坏和偷窃。



- DDOS攻击威胁:
  - 以经济利益为目标的全球黑色产业链的形成，网络上存在大量僵尸网络;
  - 不法分子的敲诈勒索，同行的恶意竞争等都有可能导致企业遭受DDoS攻击;
  - 遭受DDoS攻击时，网络带宽被大量占用，网络陷于瘫痪；受攻击服务器资源被耗尽无法响应正常用户请求，严重时会造成系统死机，企业业务无法正常运行。

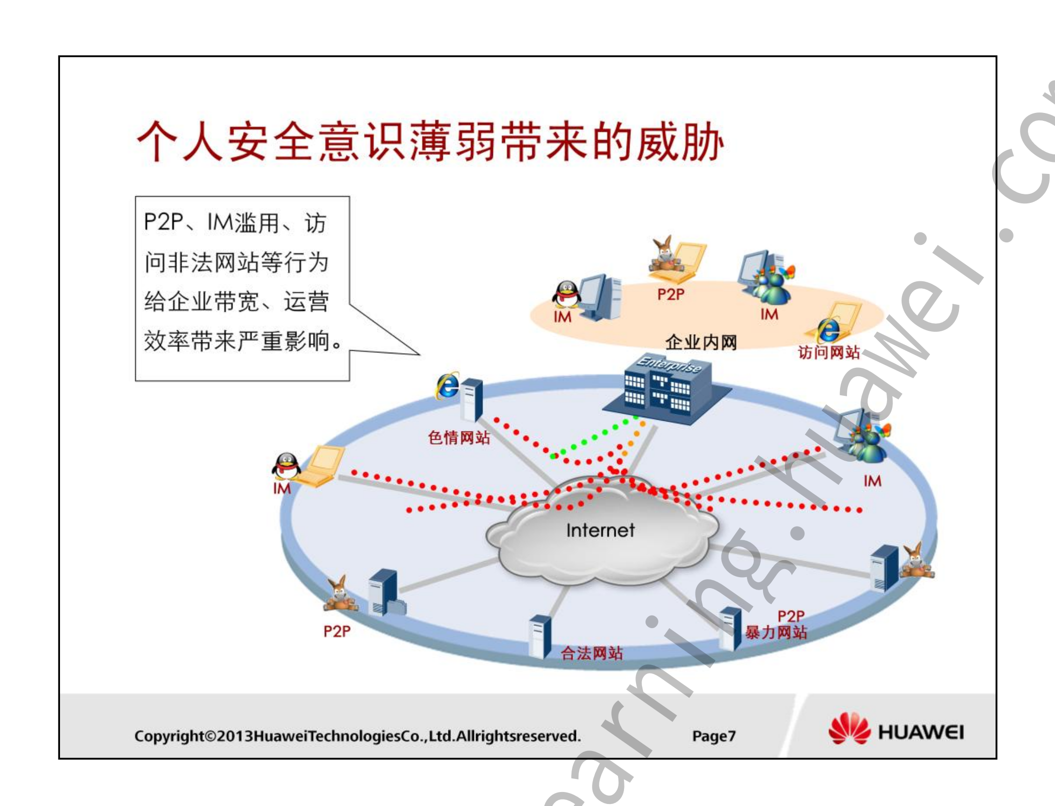
病毒及恶意软件安全威胁

- 随着企业业务拓展，更多业务应用依赖于IT信息系统来完成。在业务运行过程中，不断面临着病毒、木马、间谍软件等的严重威胁。

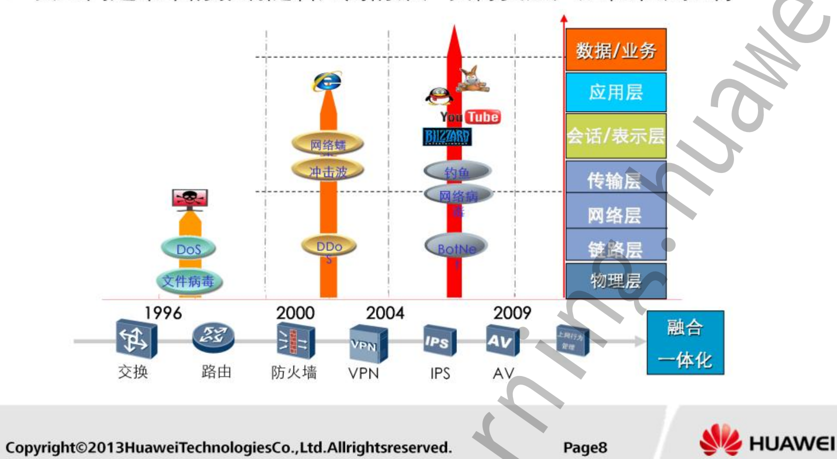
Internet
路由器
病毒
核心交换机
邮件服务器
数据服务器
Web服务器
间谍软件
木马
病毒

 Page6 HUAWEI

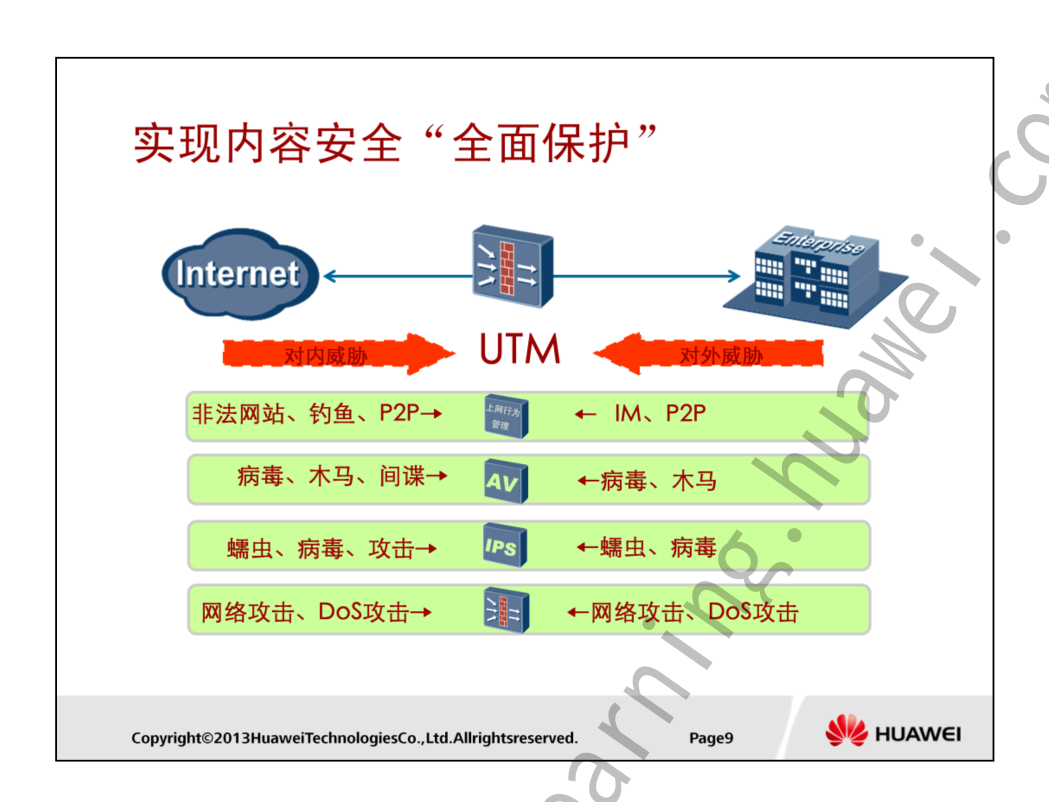
- 浏览网页、邮件传输是病毒、木马、间谍软件进入内网的主要途径；
- 病毒能够破坏计算机系统，篡改、损坏业务数据；
- 木马使黑客不仅可以窃取计算机上的重要信息，还可以对内网计算机破坏；间谍软件搜集、使用、并散播企业员工的敏感信息，严重干扰企业的正常业务；
- 桌面型反病毒软件难于从全局上防止病毒泛滥。



- P2P、IM滥用给企业带宽、运营效率带来严重影响。员工不受控Web访问可能会：
  - 被不安全的链接或者恶意下载植入代码，使机构成为僵尸网络或者感染病毒；
  - 容易被含有欺骗信息的钓鱼网站所欺骗，泄露个人银行帐号、密码等机密信息；
  - 被娱乐性内容所吸引；
  - 网页中可能带有与法律相抵触的内容（如色情、暴力），给企业带来一系列法律风险。



- 网络安全发展趋势：
  - 攻击从网络层向应用及业务层延伸，要求以网络为核心的TM技术和以终端为核心的SCM技术在网络上进行融合防范；
  - 对资源及内容的优化管理成为最关心的主题—对DPI的需求，以DPI技术为核心的业务应用将成为重点；
  - 客户从设备需求到服务需求的转化，SCTM/DPI等产品的应用要求持续提供升级及响应服务，使得商业模式发生演化；
  - 从网络安全向安全网络转化，芯片、软件技术的发展使得网络产品和安全产品的融合成为可能，广域网安全、多台网关设备集中管理、TCO等需求必将驱使路由器与安全产品融合，建设安全的网络成为基本要求。



UTM（Unified Threat Management）统一威胁管理，融合了IPS入侵防御系统、AV网关防病毒、上网行为管理、防DDOS攻击等特性，为更好的解决来自企业内部、外部的攻击威胁提供了强有力的保障。



目录



什么是入侵？

- 入侵是指未经授权而尝试访问信息系统资源、篡改信息系统中的数据，使信息系统不可靠或不能使用的行为；
- 入侵企图破坏信息系统的完整性、机密性、可用性以及可控性。

问题1：病毒是入侵行为么？

问题2：网络钓鱼是入侵行为么？

 Page11



- 典型的入侵行为：
  - 篡改Web网页；
  - 破解系统密码；
  - 复制/查看敏感数据；
  - 使用网络嗅探工具获取用户密码；
  - 访问未经允许的服务器；
  - 其他特殊硬件获得原始网络包；
  - 向主机植入特洛伊木马程序。
- 什么是网络钓鱼？
  - 网络钓鱼英文叫Phishing，是Fishing和Phone的结合体，这是因为最初的钓鱼作案就是使用的电话，所以使用Ph代替F，创造了“Phishing”这个词。
  - 网络钓鱼利用欺骗性的电子邮件和伪造的Web站点来进行诈骗活动，诈骗者把自己伪装成知名的网站、银行、在线零售商等吸引受害者上当。受害者可能在这些欺骗网站上泄露自己的银行卡账号、密码等敏感信息。

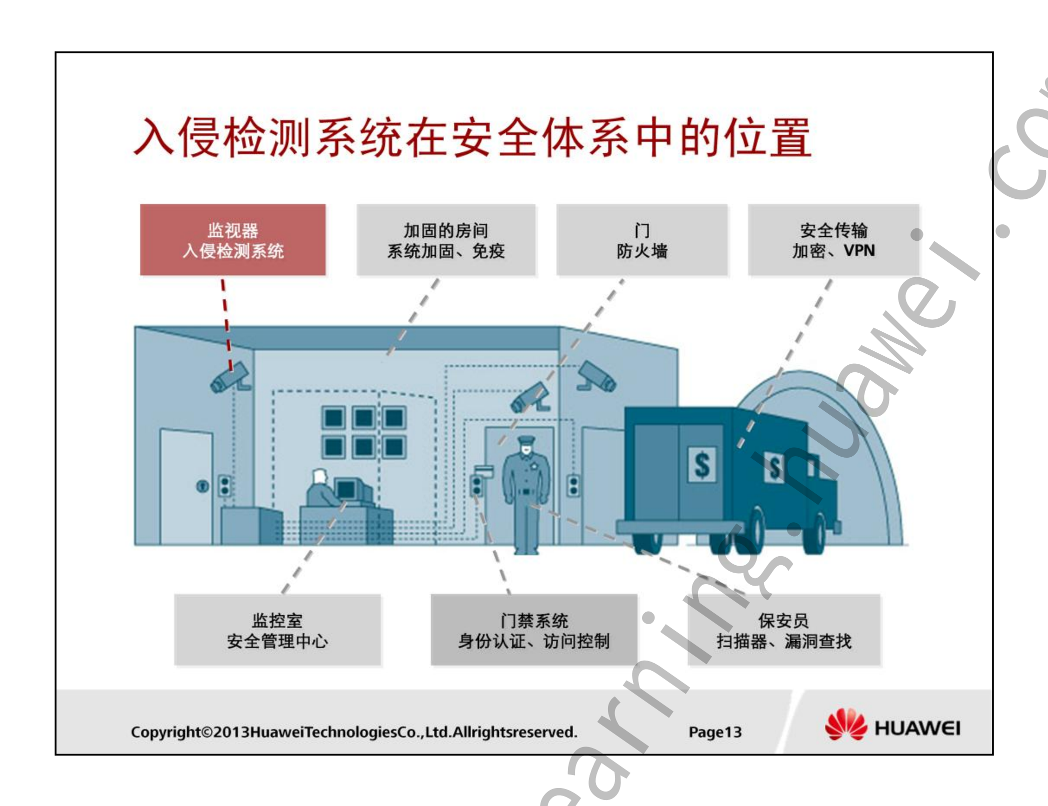
入侵检测及入侵检测系统

- 入侵检测（ID，Intrusion Detection）
  - 通过监视各种操作，分析、审计各种数据和现象来实时检测入侵行为的过程，它是一种积极的和动态的安全防御技术；
  - 入侵检测的内容涵盖了授权的和非授权的各种入侵行为。
- 入侵检测系统（IDS，Intrusion Detection System）
  - 用于入侵检测的所有软硬件系统；
  - 发现有违反安全策略的行为或系统存在被攻击的痕迹，立即启动有关安全机制进行应对。

 Page12 

入侵检测的内容涵盖了授权的和非授权的各种入侵行为，例如，违反安全策略行为、冒充其他用户、泄露系统资源、恶意行为、非法访问，以及授权者滥用权力等。

入侵检测系统可以通过网络和计算机动态地搜集大量关键信息资料，并能及时分析和判断整个系统环境的目前状态，一旦发现有违反安全策略的行为或系统存在被攻击的痕迹等，立即启动有关安全机制进行应对，例如，通过控制台或电子邮件向网络安全管理员报告案情，立即中止入侵行为、关闭整个系统、断开网络连接等。



在信息安全建设中，入侵检测系统扮演着监视器的角色，通过监控信息系统关键节点的流量，对其进行深入分析，发掘正在发生的安全事件。一个形象的比喻就是：IDS就像安全监控体系中的摄像头，通过IDS，系统管理员能够捕获关键节点的流量并做智能的分析，从中发现异常、可疑的网络行为，并向管理员报告。

- 防火墙与IDS
  - 防火墙属于串路设备，需要做快速转发，无法做深度检测；
  - 防火墙无法正确分析掺杂在允许应用数据流中的恶意代码 ，无法检测来自内部人员地恶意操作或误操作；
  - 防火墙属于粗粒度的访问控制，IDS属于细粒度的检测设备，通过IDS可以更精确地监控现网；
  - IDS可与防火墙、交换机进行联动，成为防火墙的得力“助手”，更好、更精确的控制外域间地访问；
  - IDS可灵活、及时的进行升级，策略地配置操作方便灵活。

入侵防御系统

- 入侵防御系统（IPS，Intrusion Prevention System）
  - 发现入侵行为时能实时阻断的入侵检测系统。
  - IPS使得IDS和防火墙走向统一
  - IPS在网络中一般有两种部署方式

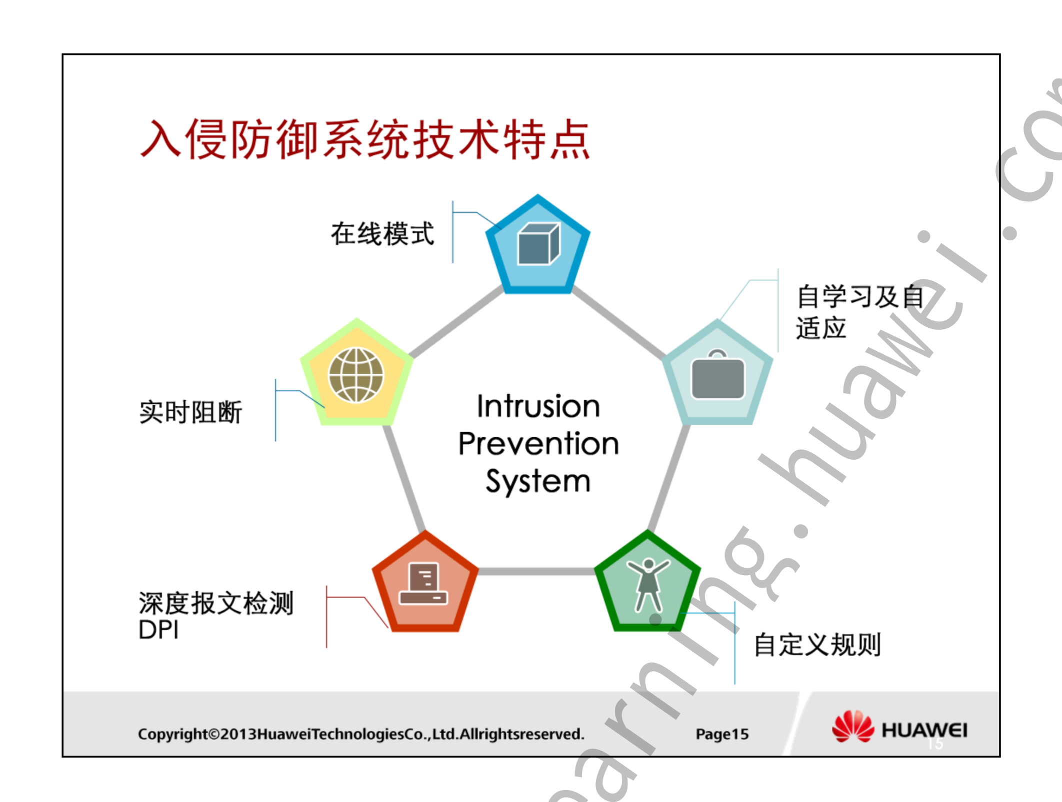
旁路	**SPAN:接在交换机上，通过交换机做端口镜像。** **TAP:通过专用的流量镜像设备，部署在网络边界。**
直路	**Inline:串接在网络边界，在线部署，在线阻断。**

 Page14 

入侵防御系统（IPS，Intrusion Prevention System），在发现入侵行为时能实时阻断的入侵检测系统。IPS是一种智能化的入侵检测和防御产品，它不但能检测入侵的发生，而且能通过一定的响应方式，实时地中止入侵行为的发生和发展，实时地保护信息系统不受实质性的攻击。

SPAN也叫做端口镜像或者端口监控，是通过交换机配置将某个端口或某组端口的流量复制到另外的端口实现的。

TAP是Test Access Point的首字母缩写，粗浅的说，Tap的概念类似于“三通”的意思，即原来的流量正常通行，同时分一股出来供监测设备分析使用。对Tap这个词的翻译，比较通用就是分光器/分路器。分光是数据通过光纤传输；分路是数据通过网线传输。其实这只是最简单的Tap的概念，目前的技术发展已经产生出很多种的Tap：有可以把多条链路汇聚起来的Tap、有把一条链路流量分成几份的Tap、有过滤Tap、有Tap switch等等，已经不能再用“三通”这个词去简单概括了。Tap的出现是整个监控/监测领域的巨大革命，它从根本上改变了监测分析系统的接入方式，使得整个监测系统有了完整灵活的解决方案。



入侵防御系统的基本技术特点主要包括：

- 在线模式（Inline）：
  - 能够让IPS实时阻断到发现的网络攻击行为，避免IDS发现攻击，而无法实时阻止攻击行为发生的缺陷，最大限度的提升系统的安全性；
- 自学习与自适应：
  - IPS能够通过自学习与自适应将系统的漏报与误报降低到最低，减少对业务的影响；
- 自定义规则：
  - IPS能够自定义入侵防御规则，最大限度的对最新的威胁作出反应；
- 深度报文检测：
  - 让IPS能够检测到基于应用层的异常与攻击；
- 实施阻断：
  - IPS因为采取的是在线部署方式，所以能够在发现攻击的同时实时阻断攻击，最大限度的提高了保护对象的安全性。



目录



计算机病毒基本概念

- 计算机病毒
  - 编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码被称为计算机病毒（Computer Virus）。
- 恶意代码
  - 一种程序，它通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序、破坏被感染电脑数据的安全性和完整性的目的。

 Page17 

计算机病毒具有破坏性，复制性和传染性。木马、间谍软件、蠕虫、逻辑炸弹、漏洞利用程序、垃圾邮件发送器、下载器、拨号器、泛洪攻击器、击键记录器均属于恶意代码，严格意义上讲计算机病毒是恶意代码的一种。

计算机病毒分类：

- 按照恶意代码功能分类：蠕虫、木马；
- 按照传播机制分类：可移动媒体、网络共享、网络扫描、电子邮件、P2P网络；
- 按照感染对象分类：操作系统、应用程序、设备；
- 按照携带者对象分类：可执行文件、脚本、宏、引导区；

病毒、蠕虫和木马

项目	病　毒	蠕　虫	木马
存在形式	寄生	独立个体	有寄生性
复制机制	插入宿主程序中	自身拷贝	不自我复制
传染性	宿主程序运行	系统存在漏洞	依据载体或功能
传染目标	主要是针对本地文件	针对网络上其它计算机	肉机或僵尸
触发机制	计算机使用者	程序自身	远程控制
影响重点	文件系统	网络性能、系统性能	信息窃取或拒绝服务
防治措施	从宿主程序中摘除	为系统打补丁(Patch)	防止木马植入



网关防病毒主要实现方式

- 代理扫描方式
  - 将所有经过网关的需要进行病毒检测的数据报文透明的转交给网关自身的协议栈，通过网关自身的协议栈将文件全部缓存下来后，再送入病毒检测引擎进行病毒检测。
- 流扫描方式
  - 依赖于状态检测技术以及协议解析技术，简单的提取文件的特征与本地签名库进行匹配。

Page19



目前设备厂商（包括UTM、AVG）的AV扫描方式，分为两种：流扫描方式和代理扫描方式。

基于代理的反病毒网关可以进行更多如解压，脱壳等高级操作，检测率高，但是，由于进行了文件全缓存，其性能、系统开销将会比较大。基于流扫描的反病毒网关性能高，开销小，但该方式检测率有限，无法应对加壳、压缩等方式处理过的文件。

网关防病毒典型技术

- 文件识别技术
- 脱壳技术
- 解压技术
- 静态识别技术
- 动态虚拟机技术





 Page20 HUAWEI

识别文件类型是检测病毒的重要手段之一。利用文件识别技术能够准确识别出文件的类型。识别一个文件的类型有多种方式，如根据后缀名或文件的真实内容。后缀名是允许用户修改的，因此并不可靠，根据文件真实内容识别则更加可靠，文件真实类型的识别一般可以由文件的前64字节就可以判断出。

实际应用中，恶意代码为了隐藏自己通常会加壳。为了使病毒检测引擎能够检测出恶意代码中的特征，病毒检测引擎需要利用脱壳技术首先进行脱壳操作。

对于压缩过的文件无论是入侵检测系统还是病毒检测系统都无法直接检测，因此需要解压技术对文件先进行解压，然后再实施病毒检测操作。

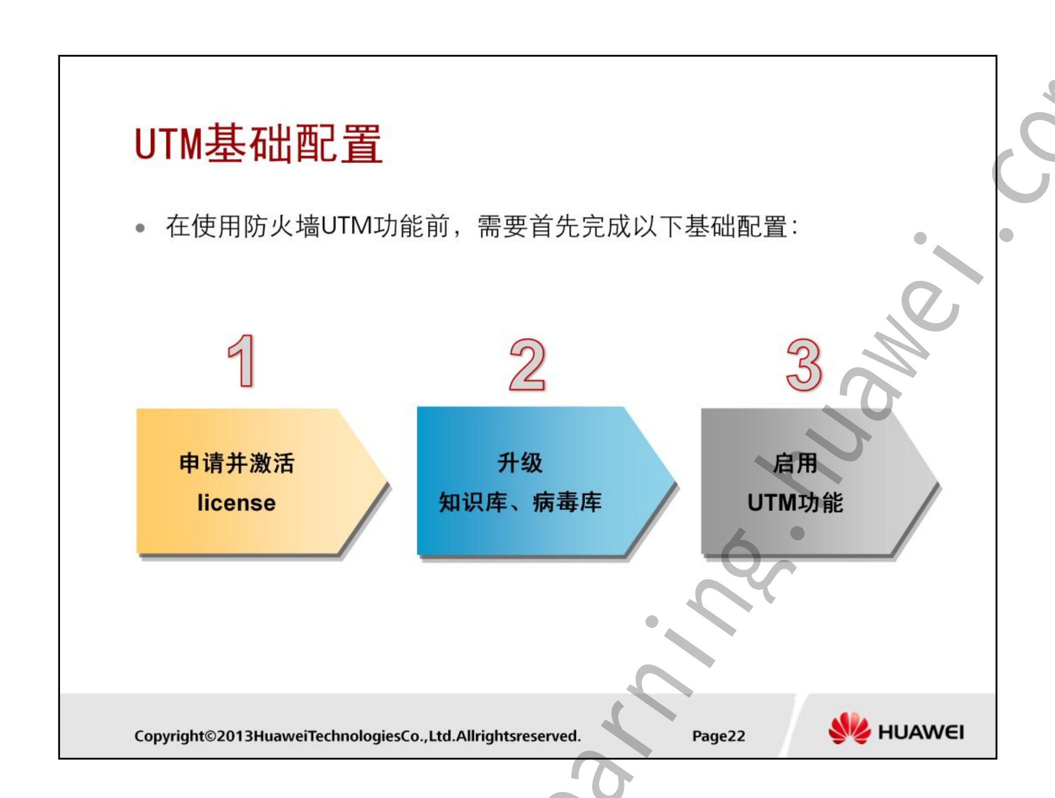
利用静态识别技术从病毒体内提取的原始数据片断，以及该片断的位置信息可以实现快速的静态分析，病毒检测的精确度高，误报少。

利用动态虚拟机技术，首先提供一个完全模拟x86指令集的可执行受管理程序的虚拟执行环境，让待检测的程序直接在该环境中执行一些指令，从而实现病毒的动态检测。



目录

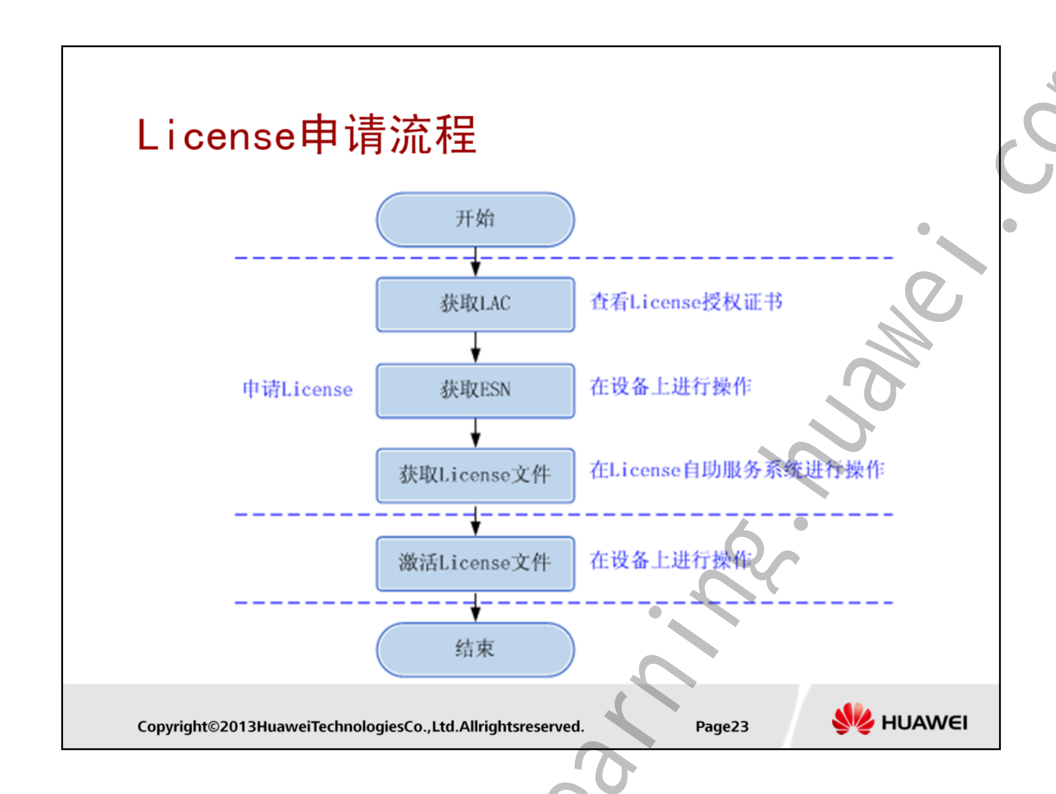




UTM功能需要License支持，在进行UTM功能配置前，需要申请并激活UTM特性的license。

使用反病毒、IPS、URL分类、应用控制功能前，首先应该指定使用的病毒库、IPS签名库、URL热点库和知识库。病毒库、IPS签名库和URL热点库需要激活License后（知识库不需要激活License），才可对其进行安装和升级。

使用UTM各功能前，必须启用UTM。



- 获取LAC

  LAC（License授权码）需要从License授权证书上获取，由数字、字母或中划线组成，长度为21位。

- 获取ESN

  ESN（设备序列号）需要在设备上进行操作获取。

- 获取License文件

  推荐通过License自助服务系统获取，也可以通过邮件方式获取。

激活license操作

- 进入"系统→维护→License管理"，激活License。

系统 > 维护 > License管理

License管理

License激活方式 ◉ 在线自动激活 ○ 本地手动激活

License中心域名 lic.huawei.com *

License授权编码 *

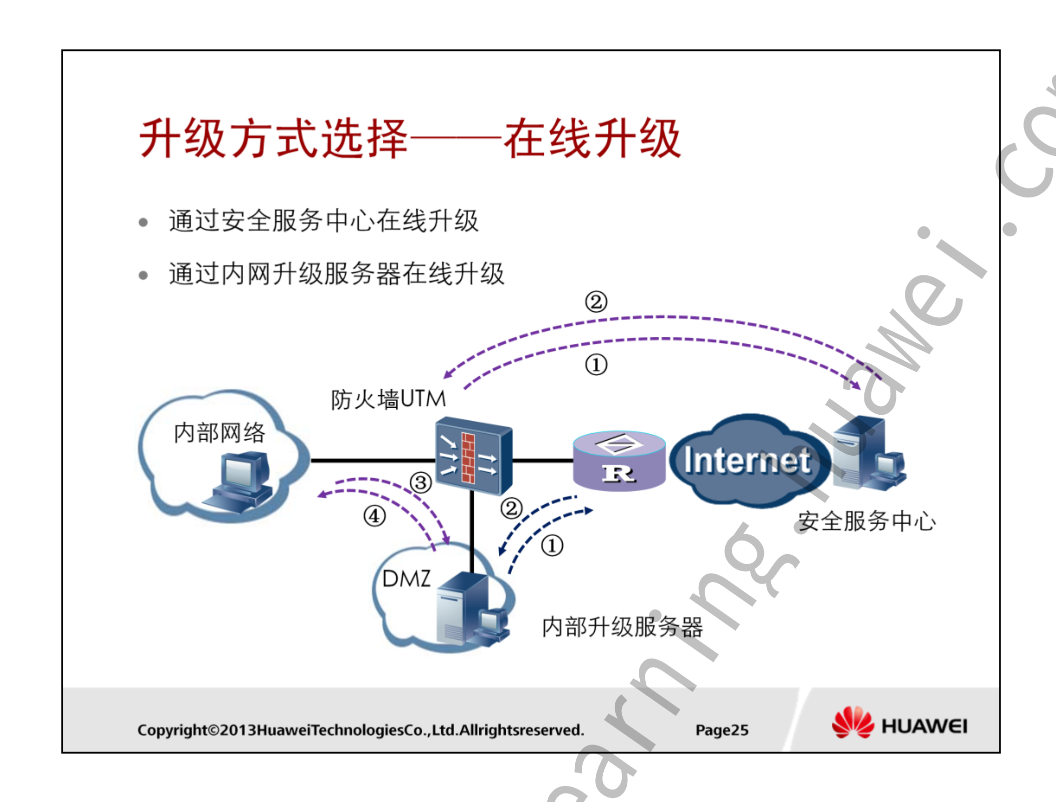
激活

License资源	状态	
虚拟防火墙	已授权（10个虚拟防火墙）	
SSL_VPN	已授权（3个并发用户）	
入侵防御	未授权（未激活）	
版本号：	0.000	[升级配置]
签名库版本：	0.000（升级时间：：00:00:00 0000/00/00）	
反病毒	未授权（未激活）	
版本号：	0.000	[升级配置]
签名库版本：	0.000（升级时间：：00:00:00 0000/00/00）	
垃圾邮件过滤	未授权（未激活）	
URL预定义分类查询	未授权（未激活）	[激活]

 Page24 HUAWEI

在激活License前，确保获取到的License文件已保存到USG的存储设备的根目录中（后缀名必须为.dat）。系统中只能存在一个处于激活状态的License文件，激活新的License将会使旧的License失效。

只有当设备ESN、软件版本等信息完全与License文件内容吻合的情况下，License才能成功被激活。



在线升级指USG连接到安全服务中心或内网升级服务器下载升级版本。

- 通过安全服务中心在线升级主要步骤:
  1. 发送更新请求、升级权限验证
  2. 下载签名库、病毒库
- 通过内网升级服务器在线升级
  1. 定期发送下载IPS版本、AV版本请求
  2. 下载IPS版本、AV版本
  3. 发送升级请求，验证升级权限和有效期
  4. 从内网升级服务器下载新版本

在线升级又分为定时在线升级和手工在线升级。

- 定时在线升级

USG定期连接安全服务中心或内网升级服务器检查是否存在新的签名库版本、病毒库版本。如果安全服务中心或内网升级服务器上存在新版本的签名库版本、病毒库版本，USG会根据设定的时间下载并更新本地的签名库或病毒库。

- 手动在线升级

当用户发现网络上出现新的攻击方式，而USG定时更新时间还没达到，或USG未启用定时更新，则需手动升级。

升级方式选择——本地升级

升级

在线升级

☑ 定时在线升级 手动在线升级

◉ 每日 03 : 05 *

○ 每周

本地升级

文件 选择

本地升级

上传文件

当前SD卡总空间：1952012 KB剩余空间：1951684 KB

文件 浏览...

导入 关闭

 Page26 HUAWEI

当USG与Internet物理隔离，且企业内网没有部署内网升级服务器时，可以采用本地升级方式。如果USG无法访问安全服务中心时，用户可以在能够访问安全服务中心的PC上手工下载升级包，上传到USG中进行本地升级。

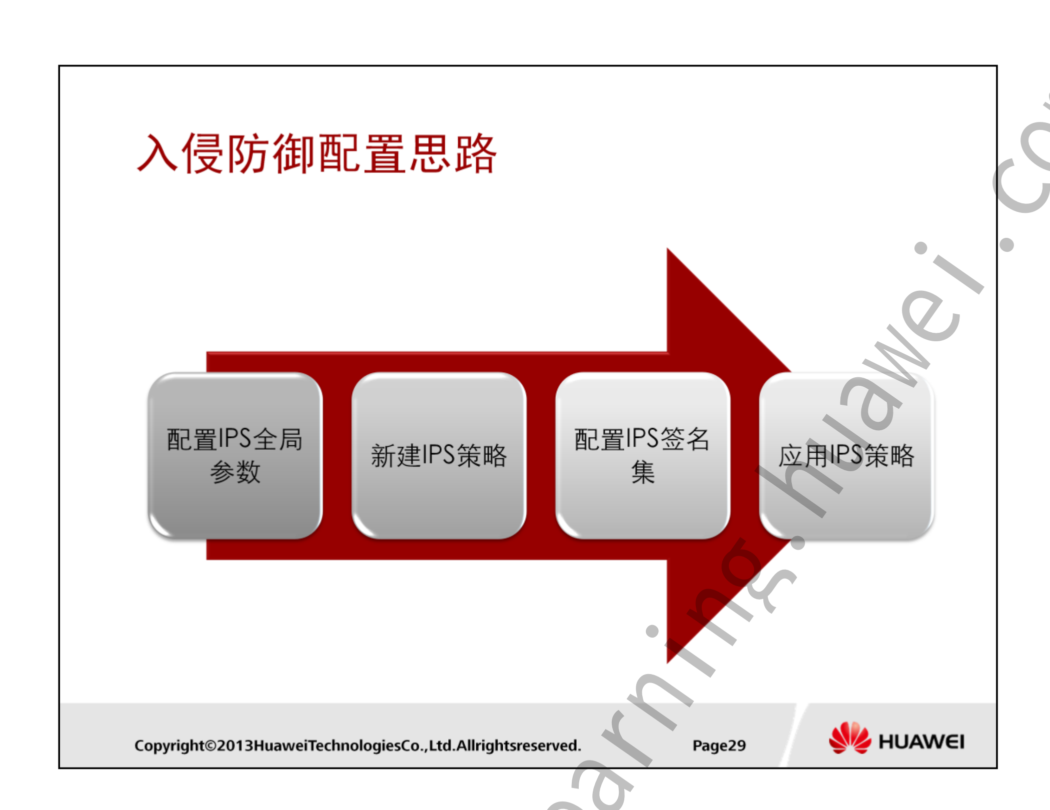


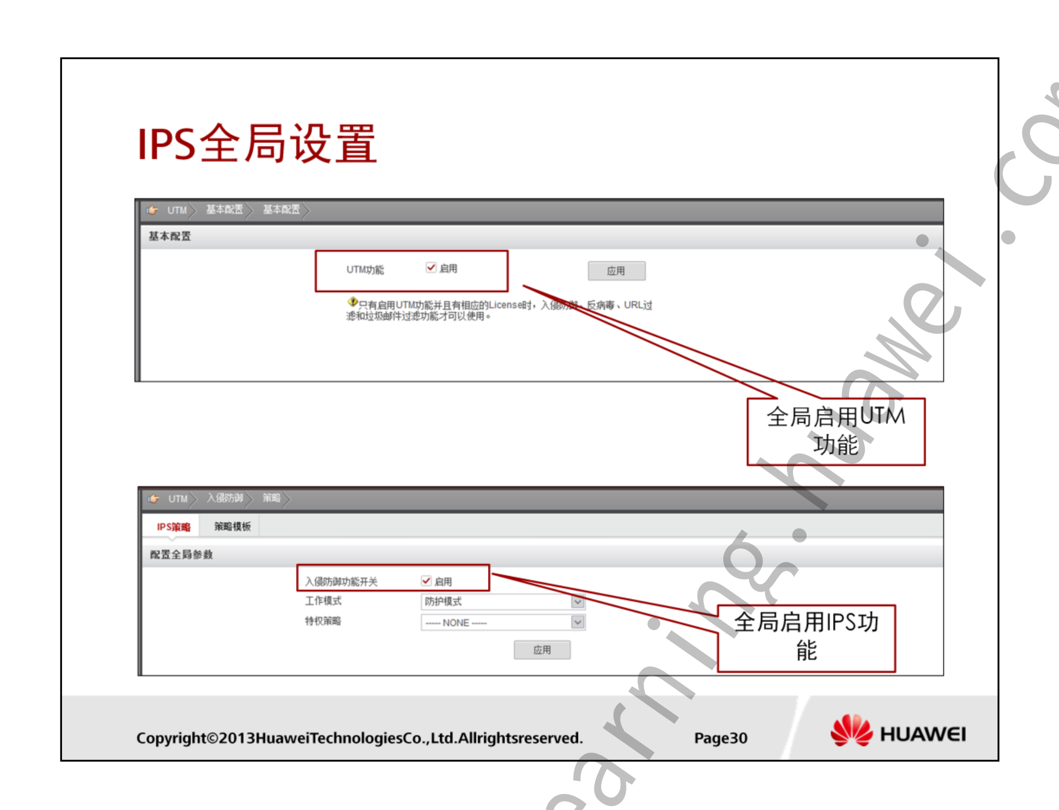
使用UTM各功能前，必须将运行模式配置为UTM模式。USG防火墙出厂默认工作在防火墙模式，也可以通过命令runmode utm，更改为UTM运行模式。



目录

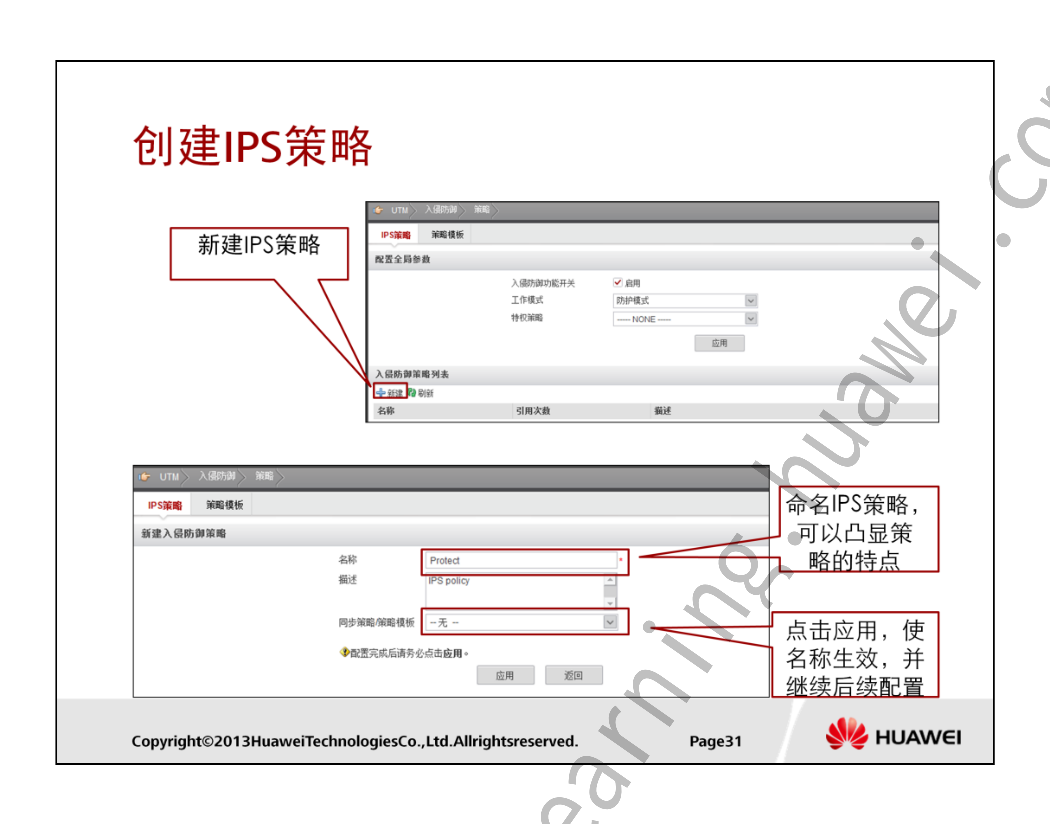



入侵防御配置思路
配置IPS全局参数
新建IPS策略
配置IPS签名集
应用IPS策略
Copyright©2013HuaweiTechnologiesCo.,Ltd.Allrightsreserved.
Page29
HUAWEI



IPS工作模式有防护模式和告警模式两种。只有在防护模式下，IPS策略中配置的阻断响应方式才可以生效；告警模式下，IPS策略中配置的阻断响应方式无效，即使报文命中的签名对应的响应方式为Block，USG5000也只会产生告警。缺省情况下，IPS工作模式为防护模式。

当网络中某一类攻击集中爆发时，需要使用统一的策略应对；当这类攻击过去，需要恢复原来配置的策略，这时可以使用特权策略。配置了特权策略后，特权策略将替换所有已经应用在域内或域间的策略。取消特权策略配置后，将恢复域内或域间原来的策略配置。



在创建IPS策略时，如果策略模板能够满足应用场景或者与应用场景相似，则可直接在策略中引用模板或引用模板后对签名集进行相应的修改。这样可以达到攻击检测率、性能最优化，同时简化配置。

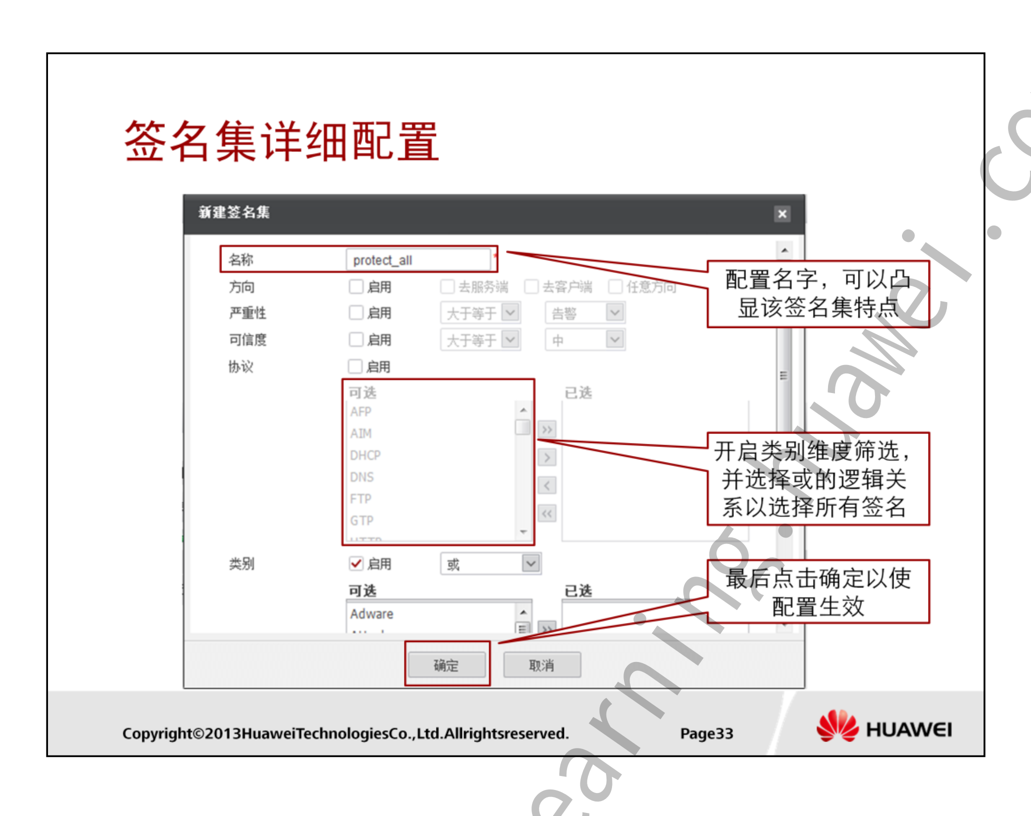
系统已经提供了以下策略模板：

- Default：默认模板。该模板可以应用在一般的入侵防御场景中。
- Ids：该模板适用于当设备以IDS（旁路）模式部署时的通用场景。
- Dmz：该模板适用于当设备部署在DMZ区域前的场景。
- web_server：该模板适用于当设备部署在Web服务器前面的场景。
- mail_server：该模板适用于当设备部署在Mail服务器前面的场景。
- dns_server：该模板适用于当设备部署在DNS服务器前面的场景。
- file_server：该模板适用于当设备部署在File服务器前面的场景。



创建IPS策略后，用户可通过配置签名集，以及签名集的启用状态和响应方式来满足特定需求。

IPS策略中配置签名集后，还可以通过配置覆盖签名满足用户的特殊需求。



创建一个签名集后，缺省情况下所有预定义签名都包含在该签名集中。用户需要以下操作过滤签名集中包含的签名：

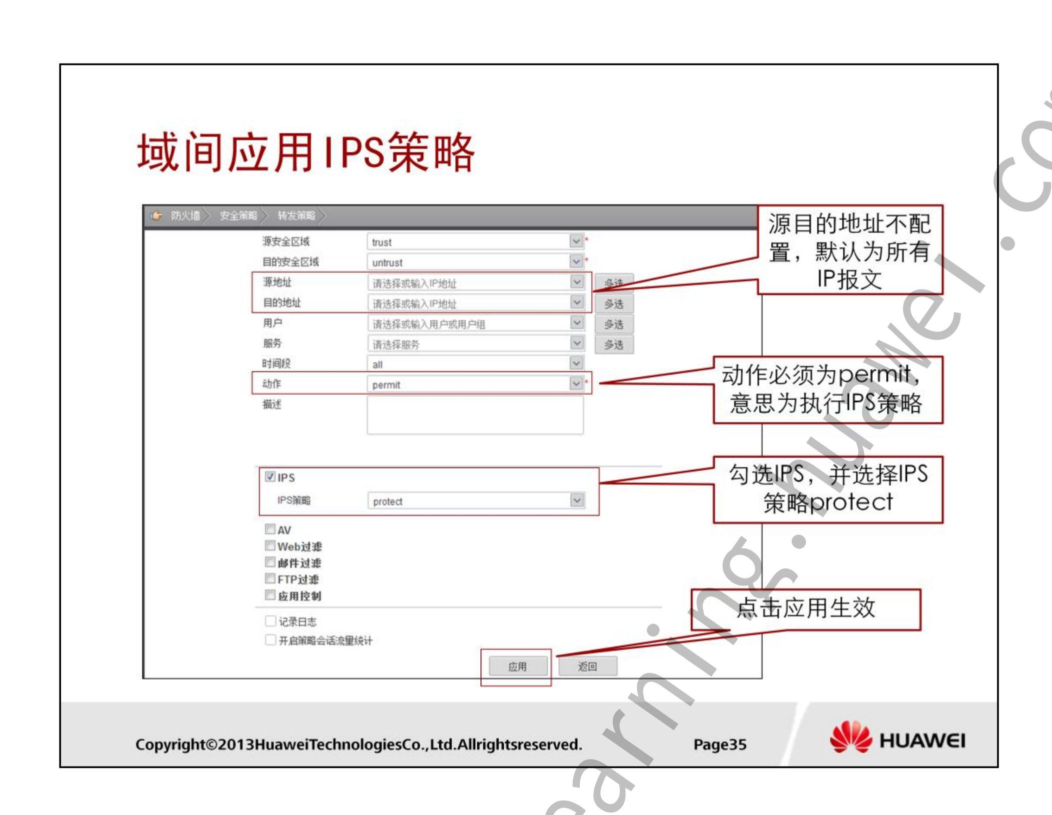
- 在签名集中启用某个过滤条件。
- 配置该过滤条件的过滤参数。
- 一个签名必须同时满足所有过滤条件才能加入签名集。

签名集中只包含预定义签名，不包含自定义签名。

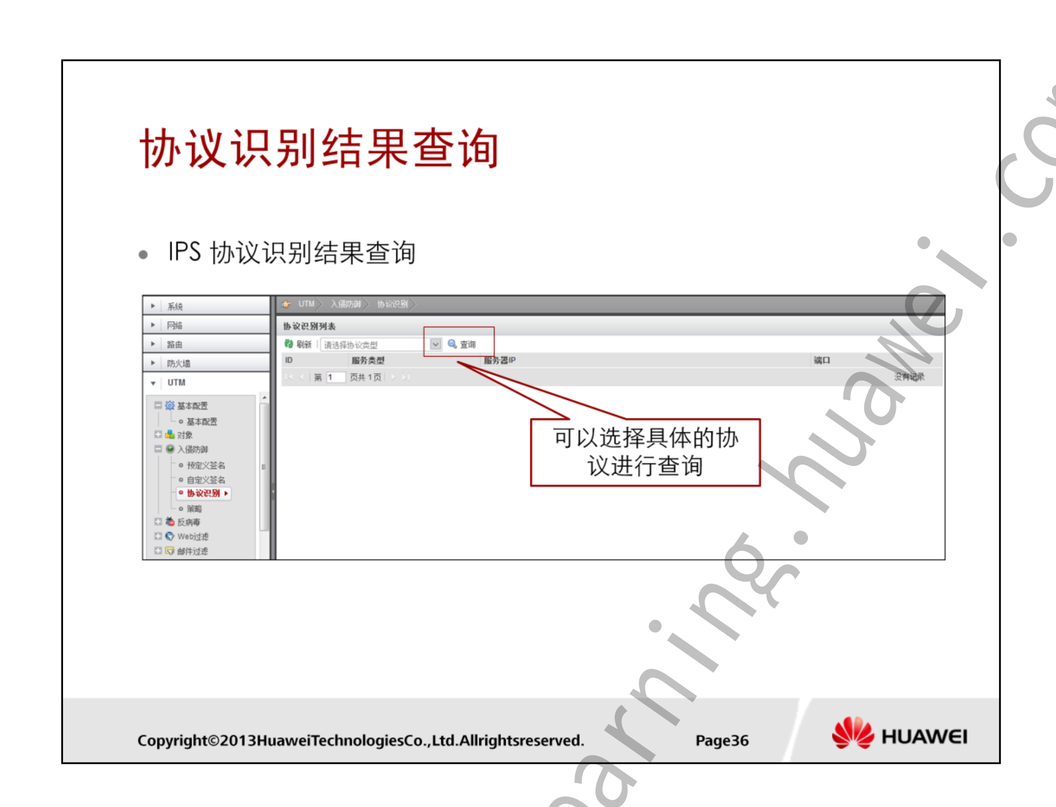


签名集之间存在优先关系，在同一条IPS策略中，排在前面的签名集比排在后面的签名集的优先级高。如果一个签名包含在一条IPS策略的多个签名集中，则按照优先级高的签名集所配置的启用状态和响应方式对匹配签名的报文进行处理。当安全威胁发生变化，用户可以调整签名集的优先级来满足新的安全需求。

IPS策略配置完成后，需要提交编译成功后才能生效。



配置IPS策略后，需要把该策略应用到域内或域间后IPS功能才生效。



协议识别功能对基于非标准端口的服务进行识别，其他特性利用协议识别的结果对报文进行处理。协议识别功能解决了对使用非标准端口的应用服务报文的漏报和误报。



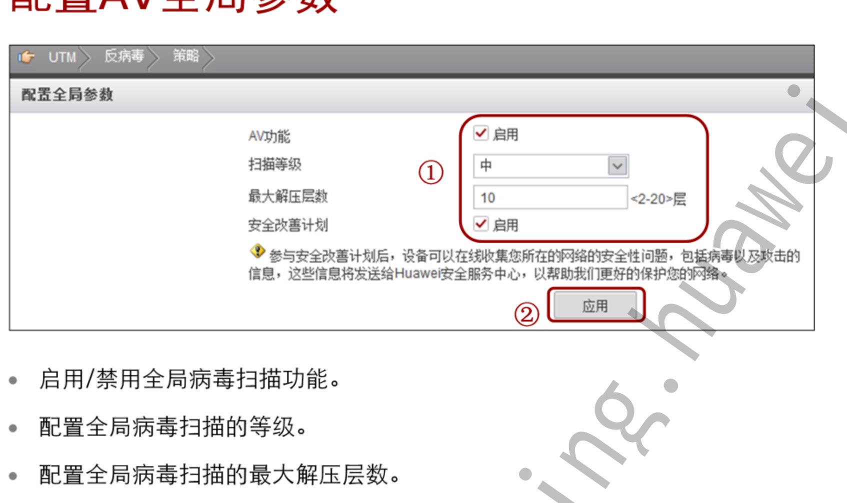
目录



网关防病毒AV配置思路

开始
升级AV病毒库（可选）
配置AV全局参数（必选）
配置AV策略（必选）
应用AV策略（必选）
结束

新建AV策略（必选）
配置AV策略的公共部分（可选）
配置HTTP协议反病毒（可选）
配置FTP协议反病毒（可选）
配置SMTP协议反病毒（可选）
配置POP3协议反病毒（可选）



 Page39 HUAWEI

- 启用/禁用全局病毒扫描功能
  - 只有启用了AV功能，应用在域间的AV策略才生效。AV功能开关只对新建连接生效，对启用AV功能之前已存在的连接不生效。
- 配置全局病毒扫描的等级
  - 扫描等级共有3级，默认为2级(中)。等级越高对文件的扫描深度越深，系统消耗的资源也越多。扫描等级取值越高，病毒检测率会越高，但产生误报的可能性也越大。改变扫描等级会导致AV引擎重新初始化。
- 配置全局病毒扫描的最大解压层数
  - 出于系统资源的考虑，超大压缩层数的设置也可以根据用户的网络现状设置，文件嵌套超过10层为压缩层数超限。
  - 当网络上传输的文件的压缩层数小于或等于最大解压层数时，文件将被解压，然后进行扫描；当文件的压缩层数大于最大解压层数时，不对文件进行扫描，并按照超过最大解压层数的动作处理。
  - 当经过设备的文件压缩层数大于最大解压层数时，设备根据AV策略公共配置的“超解压层数文件”中的处理方式丢弃或放行该文件。
- 启用/禁用安全改善计划功能
  - 启用该功能后，设备可以在线收集您所在的网络的安全性问题，包括病毒和攻击信息，并将这些信息发送给安全服务中心，以帮助我们更好的保护您的网络。

配置AV全局参数

- 配置AV全局参数
  - 选择“UTM > 反病毒 > 策略”。
  - 在“配置全局参数”区域框中配置AV全局参数。
  - 单击“应用”。

  注：AV全局参数的配置对所有AV策略都有效。
- 新建AV策略
  - 选择“UTM > 反病毒 > 策略”。
  - 单击“新建”。
  - 输入新建AV策略的名称和描述。
  - 单击“应用”。

配置AV策略的公共部分

公共配置

超大文件	允许	密码保护文件	允许
受损文件 ①	允许	超解压层数文件 ②	允许

- 超大文件
- 密码保护文件
- 受损文件
- 超解压层数文件

 Page41 HUAWEI

- 在“公共配置”区域框中配置参数。（超大文件、密码保护文件、受损文件、超解压层数文件）
  - 允许：允许文件通过，对HTTP、FTP协议传输的文件：允许文件通过，只产生日志；对SMTP、POP3协议传输的文件：允许文件通过，同时在邮件正文中添加宣告并产生日志。
  - 拒绝：阻断文件通过，对HTTP、FTP协议传输的文件：阻断文件通过，同时向客户端推送Web页面并产生日志；对SMTP、POP3协议传输的文件：阻断邮件的附件，同时在邮件正文中添加宣告并产生日志。
  - 单击“应用”，完成公共配置。

注：AV策略的公共部分对该策略的所有协议都有效。

出于系统资源的考虑，超大文件和超大压缩层数的文件，用户的配置通过还是阻断。对于密码保护的文件，由于网关设备不具备密码破解能力，因此可以由用户设定对密码保护文件的处理方式为通过还是阻断。

文件在主机上以一定的格式保存、读取和解析，对于格式损坏的文件，设备可以直接检测到，并根据用户的配置允许通过或阻断。

配置HTTP协议反病毒

HTTP协议配置

病毒扫描 ① ☑启用
HTTP传输模式 ☑上传 ☑下载
断点续传 ② ☑启用
传输体验 ☐启用
文件大小上限 1 <1-20>MB
文件扫描方式 ○智能扫描 ◉指定扩展名扫描 配置
响应方式 ③ 告警
推送内容

- 对使用HTTP协议传输的文件启用病毒扫描。
- 配置对HTTP文件进行病毒扫描的参数
- 配置响应方式及推送内容

 Page42 HUAWEI

- 在“HTTP协议配置”区域框中配置各参数。
  - 启用病毒扫描
  - HTTP传输模式
  - 断点续传：AV策略支持对断点续传的HTTP文件进行传输，但不对断点续传的HTTP文件进行病毒扫描。
  - 传输体验，启用此功能可提高文件传输速率，但有可能导致带病毒的文件漏阻断。在观看在线视频的情况下，请启用传输体验。
  - 文件大小上限。以post方式上传多个文件时，设备将根据多个文件的总大小判定是否为超大文件；当经过设备的HTTP协议文件大于最大扫描文件大小的值时，设备根据公共配置中超大文件的处理方式丢弃或放行该文件。
  - 文件扫描方式，智能扫描：根据文件的真实类型进行扫描。此方式下设备扫描所有文件；指定扩展名扫描：根据文件扩展名表示的文件类型进行扫描。
  - 响应方式，告警：设备只产生日志，不对HTTP协议传输的文件进行处理就发送出去；阻断：设备断开与HTTP服务器的连接并阻断文件，向客户端推送Web页面并产生日志
  - Web推送内容，当设备阻断文件传输时向客户端推送的Web页面内容。

配置FTP协议反病毒

FTP协议配置

病毒扫描	①	☑ 启用
FTP传输模式	②	☑ 上传 ☑ 下载
断点续传		☑ 启用
传输体验		☐ 启用
文件大小上限		1 <1-20>MB
文件扫描方式		○ 智能扫描 ◉ 指定扩展名扫描 配置
响应方式	③	告警
推送内容		The uploaded or downloaded file has security risks

- 对使用FTP协议传输的文件启用病毒扫描。
- 配置对FTP文件进行病毒扫描的参数
- 配置响应方式及推送内容

 Page43 HUAWEI

- 在“FTP协议配置”区域框中配置各参数。
  - 启用病毒扫描
  - FTP传输模式
  - 断点续传： AV策略支持对断点续传的FTP文件进行传输，但不对断点续传的FTP文件进行病毒扫描。
  - 传输体验，启用此功能可提高文件传输速率，但有可能导致带病毒的文件漏阻断。在观看在线视频的情况下，请启用传输体验。
  - 文件大小上限，当经过设备的FTP协议文件大于最大扫描文件大小的值时，设备根据公共配置中超大文件的处理方式丢弃或放行该文件。
  - 文件扫描方式，智能扫描：根据文件的真实类型进行扫描。此方式下设备扫描所有文件。 指定扩展名扫描：根据文件扩展名表示的文件类型进行扫描。
  - 响应方式，告警：设备只产生日志，不对HTTP协议传输的文件进行处理就发送出去；阻断：设备断开与HTTP服务器的连接并阻断文件，向客户端推送Web页面并产生日志。
  - Web推送内容，当设备阻断文件传输时向客户端推送的Web页面内容。



- 在“SMTP协议配置”区域框中配置各参数。
    - 启用病毒扫描
    - 文件大小上限，当经过设备的SMTP协议文件大于最大扫描文件大小的值时，设备根据公共配置中超大文件的处理方式丢弃或放行该文件。
    - 文件扫描方式，智能扫描：根据文件的真实类型进行扫描。此方式下设备扫描所有文件；指定扩展名扫描：根据文件扩展名表示的文件类型进行扫描。
    - 响应方式，告警：设备只产生日志，不对HTTP协议传输的文件进行处理就发送出去；阻断：设备断开与HTTP服务器的连接并阻断文件，向客户端推送Web页面并产生日志
    - 宣告内容（英文），此模式下配置的宣告内容只会添加到字符集是US-ASCII和UTF-7的邮件中。
    - 宣告内容（中文），此模式下配置的宣告内容只会添加到字符集是GB2312的邮件中。

配置POP3协议反病毒



- 对使用POP3协议传输的文件启用病毒扫描。
- 配置对POP3文件进行病毒扫描的参数
- 配置响应方式及宣告内容

 Page45



- 在“POP3协议配置”区域框中配置各参数。
    - 启用病毒扫描
    - 文件大小上限，当经过设备的POP3协议文件大于最大扫描文件大小的值时，设备根据公共配置中超大文件的处理方式丢弃或放行该文件。
    - 文件扫描方式，智能扫描：根据文件的真实类型进行扫描。此方式下设备扫描所有文件；指定扩展名扫描：根据文件扩展名表示的文件类型进行扫描。
    - 响应方式，告警：设备只产生日志，不对HTTP协议传输的文件进行处理就发送出去；阻断：设备断开与HTTP服务器的连接并阻断文件，向客户端推送Web页面并产生日志
    - 宣告内容（英文），此模式下配置的宣告内容只会添加到字符集是US-ASCII和UTF-7的邮件中。
    - 宣告内容（中文），此模式下配置的宣告内容只会添加到字符集是GB2312的邮件中。



- 配置完策略后，需要应用邮件过滤策略。
  - 选择“防火墙 > 安全策略 > 转发策略”。
  - 在“转发策略列表”中，单击“新建”。
  - 在“新建转发策略”区域，依次输入或选择各项参数。
  - 选中“AV”复选框，选择前面配置的相应AV策略。
  - 单击“应用”，完成AV防病毒策略应用的配置。



总结

- 防火墙UTM技术产生的背景；
- 防火墙UTM特性；
- 防火墙UTM特性配置。



练习题

- 判断题
  1. DPI技术是通过对报文的应用层数据进行内容检测，分析报文或流在IP和UDP/TCP层以上及各种隧道内部的应用类型。
  2. 开启AV功能的断点续传功能后，分块传输不再扫描，直接通过。
- 多选题
  1. 下列属于应用层常见的攻击有？

     A、缓冲区溢出 B、病毒 C、CC攻击 D、arp欺骗网

  2. AV功能支持的协议类型包括：

     A、HTTP B、FTP C、SMTP D、POP3



习题与答案：

1、DPI技术是通过对报文的应用层数据进行内容检测，分析报文或流在IP和UDP/TCP层以上及各种隧道内部的应用类型。

答案：正确

2、开启AV功能的断点续传功能后，分块传输不再扫描，直接通过。

答案：正确

3、下列属于应用层常见的攻击有？

A、缓冲区溢出B、病毒C、CC攻击D、arp欺骗

答案：ABC

4、AV功能支持的协议类型包括：

A、HTTP B、FTP C、SMTP D、POP3

答案：ABCD

Thankyou

www.huawei.com

HC110310012

HCNA-Security CBSN 第十二章 终端安全技术

第十二章 终端安全技术

www.huawei.com

HUAWEI



目标

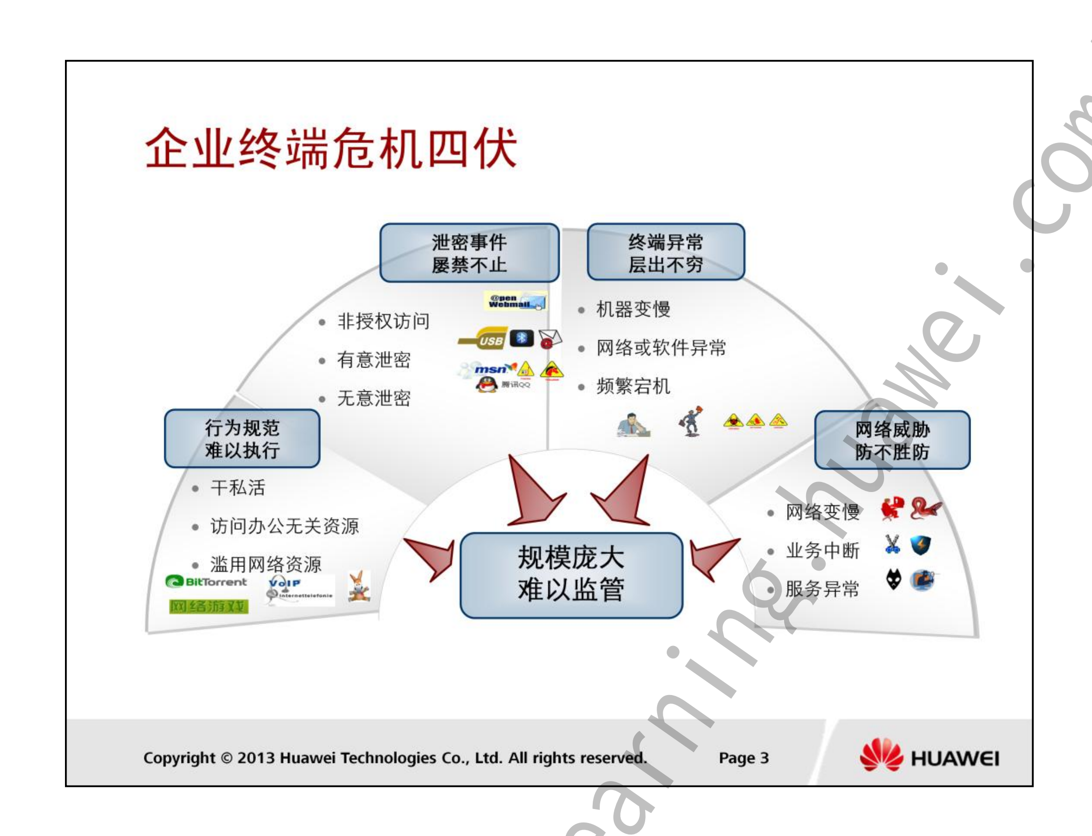
- 学完本课程后，您将能够:
  - 了解什么是终端安全
  - 掌握TSM系统的组成部分及如何部署
  - 理解TSM系统组织管理和准入控制方式
  - 掌握TSM系统的安全策略配置





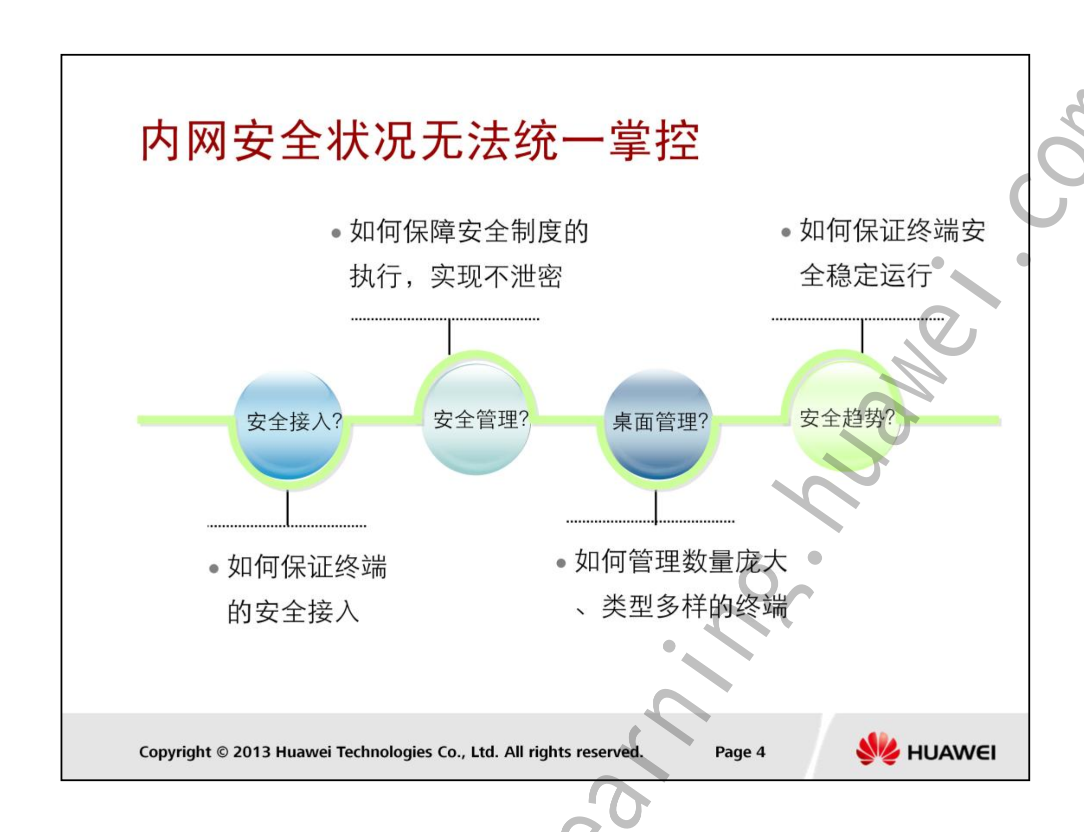
目录





企业虽然部署了杀毒软件和安全设备，但是依然存在如下问题：

- 泄密事件屡禁不止：
- 非授权访问：外来电脑、跨部门接入电脑、跨权限访问
- 有意泄密：外设拷贝、聊天、文件传输、资产外出
- 无意泄密：病毒木马蠕虫、恶意网站、资产丢失
- 终端异常层现不穷：
- 病毒、蠕虫、木马、流氓软件导致机器过慢；
- 恶意代码或入侵事件导致网络或软件异常，使得IT人员沦为疲于奔命的“救火队员
- 系统破坏、软件冲突导致频繁宕机，使得IT部门形象受损
- 网络威胁防不胜防：
- 病毒、蠕虫、源自终端的恶意攻击（入网络剪刀手、网络执法官等、ARP攻击）、网络资源滥用导致网络变慢甚至业务终端或应用系统异常



- 内网安全的诸多问题，困扰着IT管理和维护人员：
  - 休息日是否有外来终端接入?
  - 是否有不符合安全要求的终端接入?
  - 是否有越权访问重要服务器的行为?
  - 最近有没有泄密事件?
  - 本次网络事故是否由终端造成?
  - 安全制度有没有人违反?
  - 最近公司资产有没有流失？计划升级哪些硬盘?
  - 哪些终端安装了存在法律问题的软件?
  - 如何将办公软件或新补丁部署到上万台终端?
  - 分支机构的电脑出问题了，如何远程解决?
  - 信息泄密违规趋势?
  - 终端安全性和可用性趋势?
  - 安全法规、制度遵从性趋势?

终端安全现状

安全威胁出现频度对比，2007 年

病毒、特洛伊木马及恶意代码 96.1
垃圾邮件 55.9
间谍软件 33.3
应用程序的漏洞 31.6
黑客入侵 22.1
内部员工破坏IT系统 8.1
无线网络带来的安全问题 8.1
内部雇员或者合作伙伴偷窃数据 7.8

IDC统计报告

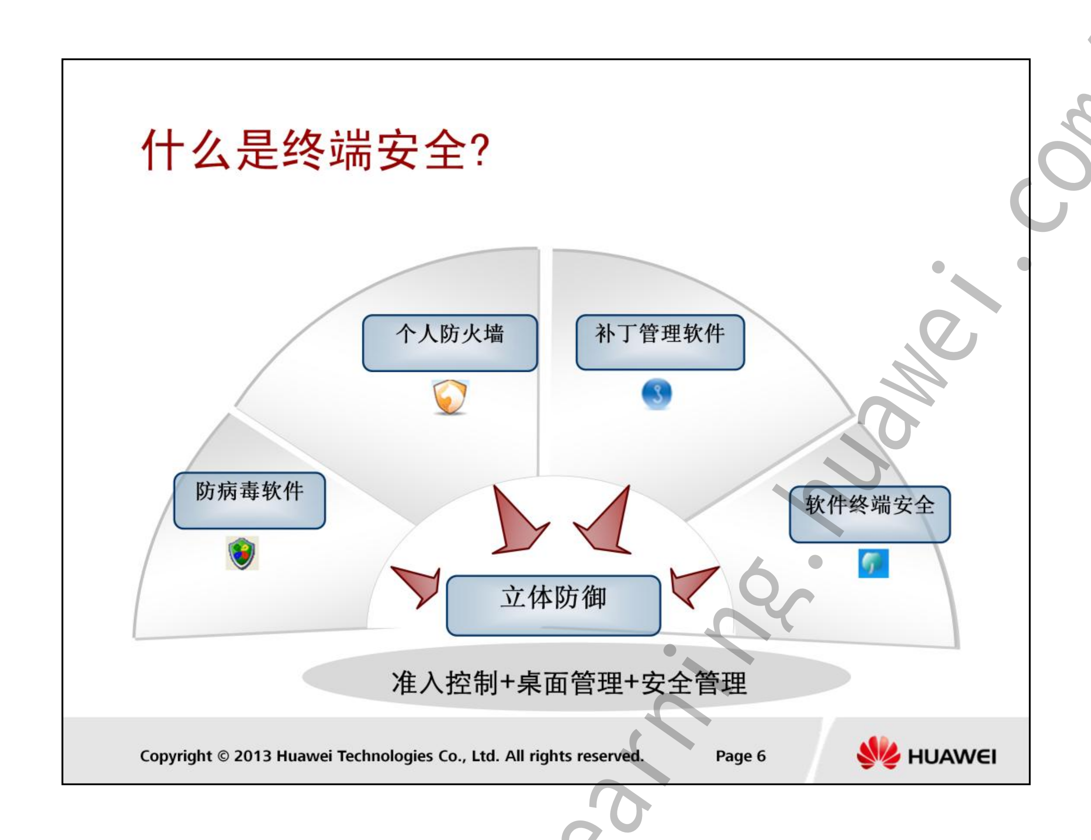
形同虚设?
Enterprise
文件服务器
邮件服务器
WEB服务器

- **内网安全主要威胁**
  - 存储介质滥用与失窃
  - 未授权访问
  - 重要信息资产泄密
  - 病毒及恶意代码

 Page 5 

据IDC统计报告和CSI/FBI 计算机犯罪与安全调查显示，存储介质滥用与失窃、未授权访问、重要信息资产泄密、IT系统漏洞、病毒及恶意代码、 IM即时通讯软件和非工作时间的Web访问已经成为企业面临的最严重的安全威胁之一。而目前企业信息安全建设现状是，企业在严防死守外部黑客和病毒攻击的同时，却忽略了内部威胁。从2大组织显示的报告得知，有大量的企业内部安全威胁正在对企业重要的信息资产造成严重的影响。

因此，传统的边界防护措施在越来越多的内网安全风险面前，呈现出“形同虚设”态势。所以，企业IT管理人员需要逐步将工作中心向内网安全防护转移。

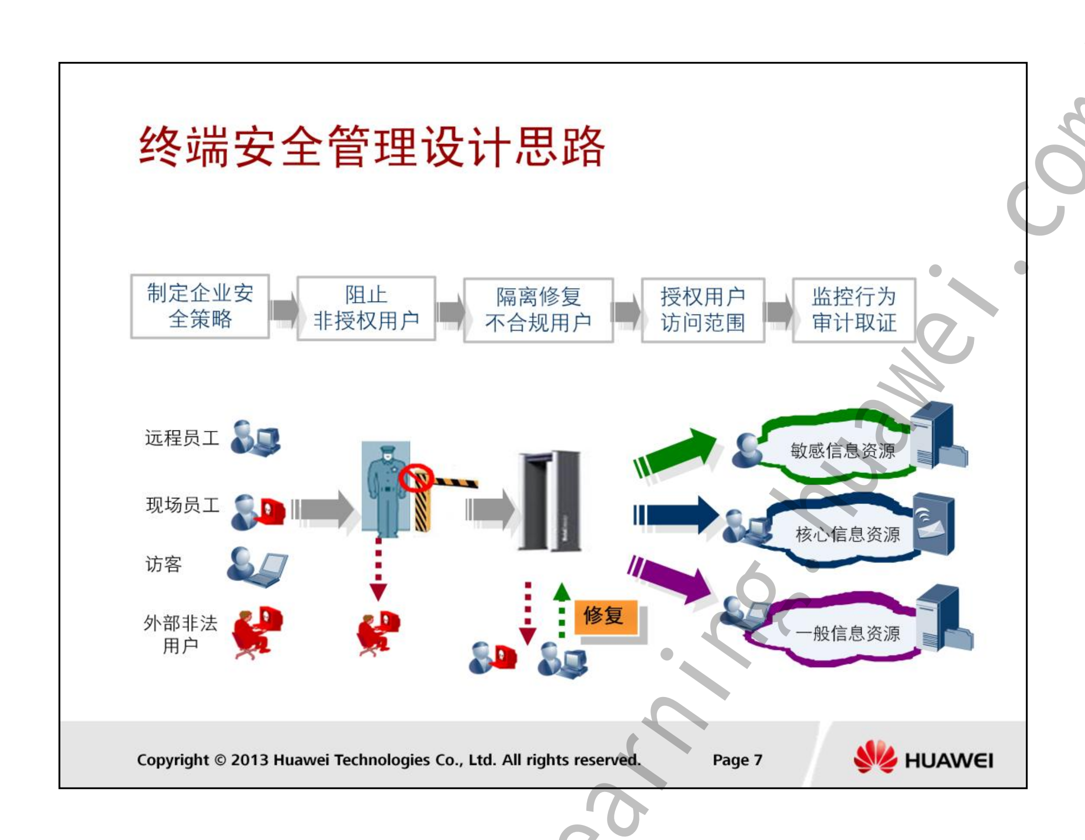


什么是终端安全？提到终端安全我们很容易联想到传统的防病毒软件、个人防火墙及补丁管理。从狭义上讲，以上可以是终端安全，但我们也看到，以上终端安全是孤立的，也就是说从广义上来讲，以上部分只能算终端安全组成部分。那么什么是终端安全？终端安全要解决哪些问题？为什么以上传统终端安全产品难以从根本上解决安全所面临的问题？

防病毒软件在20世纪80年代随着病毒产生而产生，经过近几十年的发展，已从当时的个人版发展当前的网络版、网关版。但企业部署完防病毒软件后，发现病毒感染还是大面积发生，虽然有产品自身技术局限性外，其中各终端未按网络管理人员要求进行引擎升级、病毒库升级占大多数，更有甚者某些终端长时间都未安装防病毒软件。而个人防火墙、补丁管理软件在企业部署过程中，也存在与防病毒软件类似的挑战。

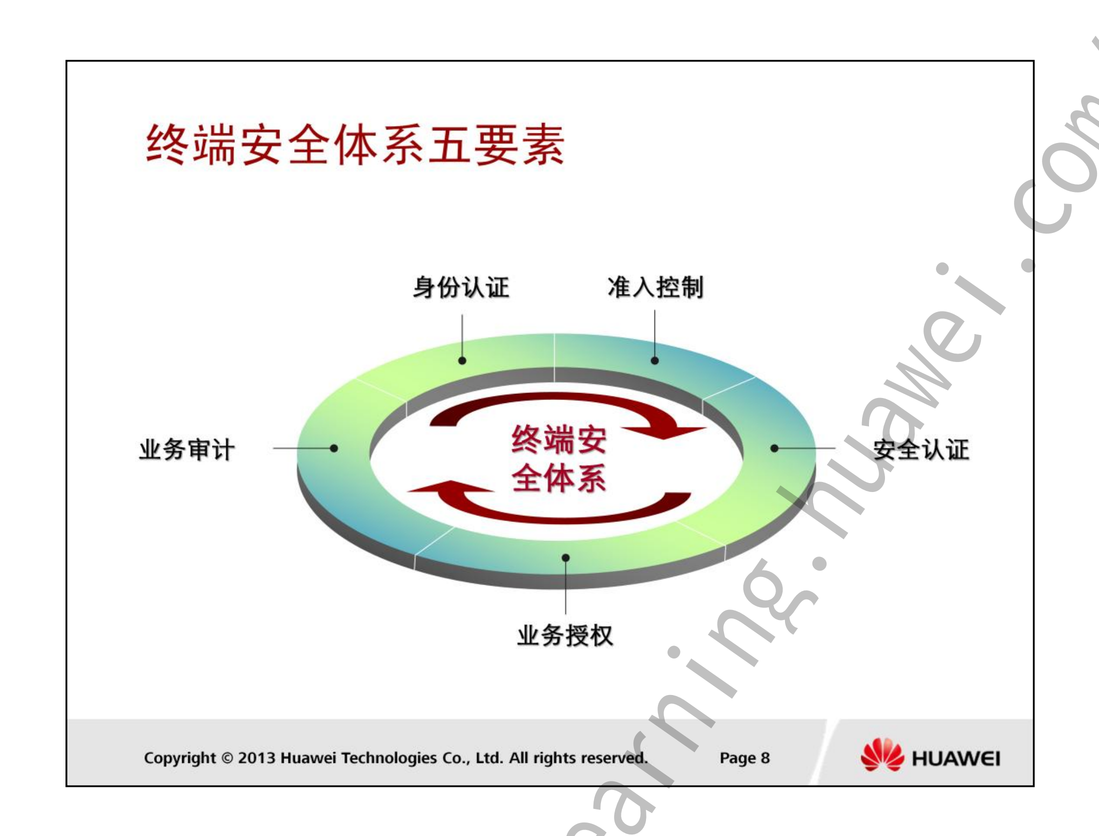
基于以上传统终端安全所面临的局限性，21世纪初期，逐步有IT厂商开发出软件类终端安全来解决所面临挑战，但在实施交付中，厂商和企业越来越感到单纯的软件类终端安全很难从体系架构层面来整体解决终端所面临的安全问题。这就促使一批具有综合技术能力的IT厂商介入终端安全领域，华为公司借助自身安全实践、网络技术开发、安全软件开发等能力，提出了终端安全立体防御解决。所谓立体防御，是指基于终端所面临的问题，对相关产品及组件进行整合，形成统一的、整体的纵深防御方案，以解决单一防护可能带来的局限性。

终端安全，是采用立体防御理念形成体系化产品与解决方案。它体现了立体架构和主动防御思想，并通过PDCA模型（P规划方案、D实施维护、C检查评估、A处理整改）来持续提升企业终端的安全能力。终端安全立体防御体系，即通过准入控制来识别终端用户身份，以决定是否允许其接入；桌面管理是通过制定相应安全策略来保障终端桌面的安全；安全管理是通过制定适合企业业务运营要求的安全管理，来确保所制定的安全策略有法可依。



现在我们来看一下终端安全管理解决方案的设计思路。

以企业安全策略为核心，用户在接入企业标准网络之前，第一步接受身份验证，认证通过后进行第二步强制合规性检查（包括安全状态和系统配置检查），服务器依据检查结果作出仲裁，符合企业安全策略即可授权访问相应的网络资源；安全检查不合规的终端只能访问修复资源，完成必要的修复后才能接入网络。代理对所有接入网络的终端进行持续的行为监控，及时对违规行为作出响应，并进行记录。整个流程形成了内网安全保护的PDCA持续改进过程。



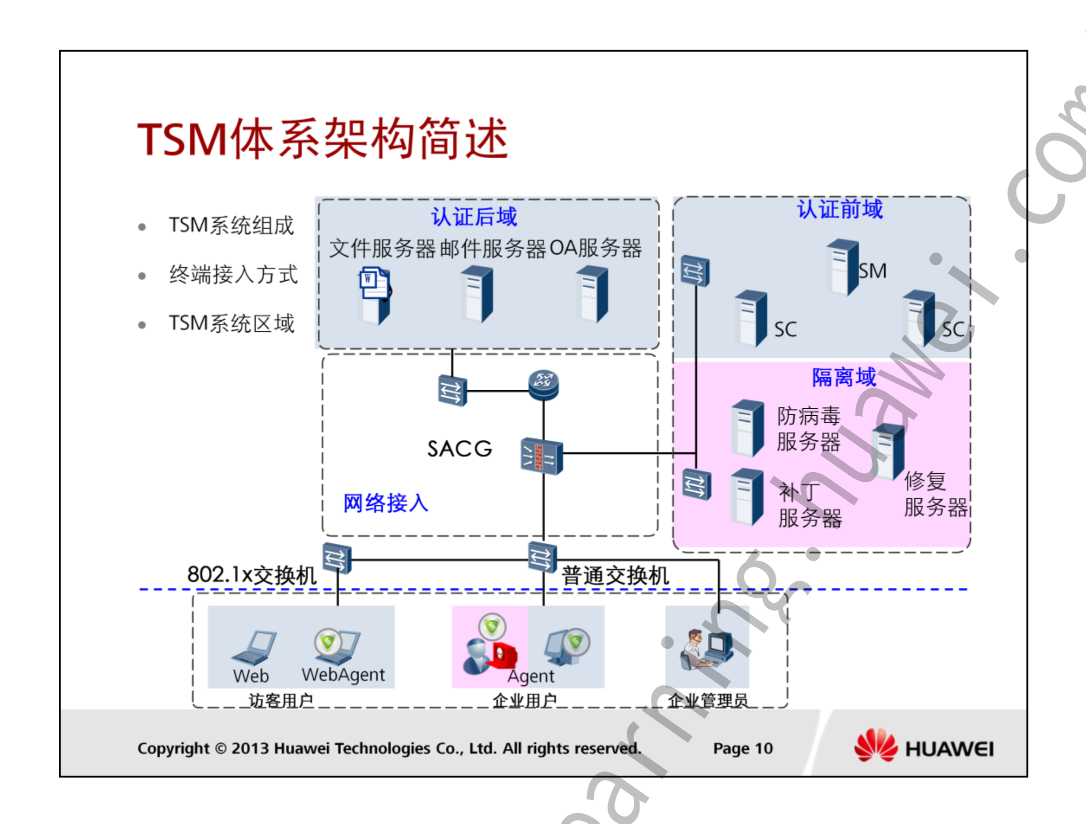
终端安全体系建立需要考虑的五个要素：

- 身份认证：关注身份标识、角色定义、外部认证系统等；
- 准入控制：关注软件防火墙、802.1X交换机、网关准入控制、ARP、DHCP；
- 安全认证：关注防病毒软件、补丁管理、非法外联管理、存储介质管理、上网行为管理等；
- 业务授权：关注业务系统权限控制、业务文档权限控制；
- 业务审计：关注业务系统类审计、业务文档类审计。



1. 终端安全概述
2. **终端安全系统部署**
3. 终端安全策略部署





1、TSM系统组成：

1）SM管理服务器；

2）SC控制服务器；

3）准入控制：硬件SACG、802.1X交换机、软件SACG；

2、终端接入方式：

1）Web，只进行身份认证；

2）WebAgent，进行身份认证和部分安全认证；

3）Agent，进行身份认证和安全认证；

3、TSM系统区域：

1）认证前域，身份认证前终端所能访问区域；

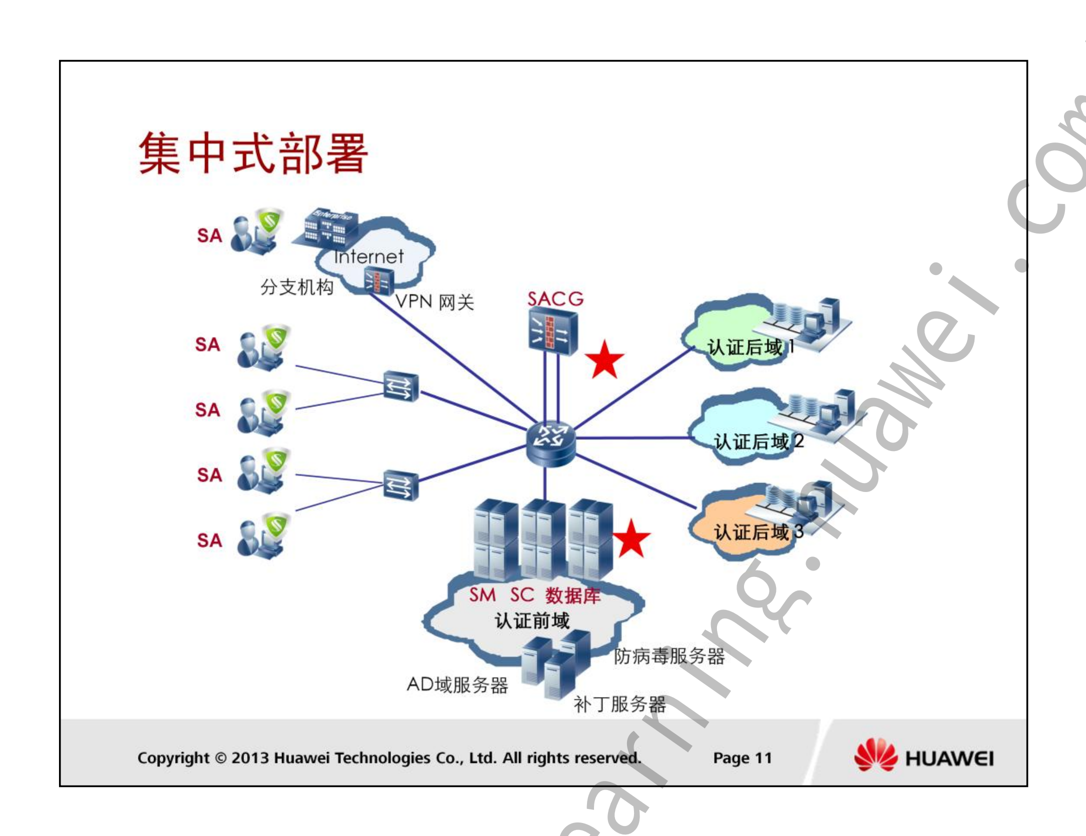
2）隔离域，身份认证后，安全认证不通过终端需进行安全修复的区域；

3）认证后域，安全认证通过后，终端基于业务需求角色所授予业务资源访问权限的区域；

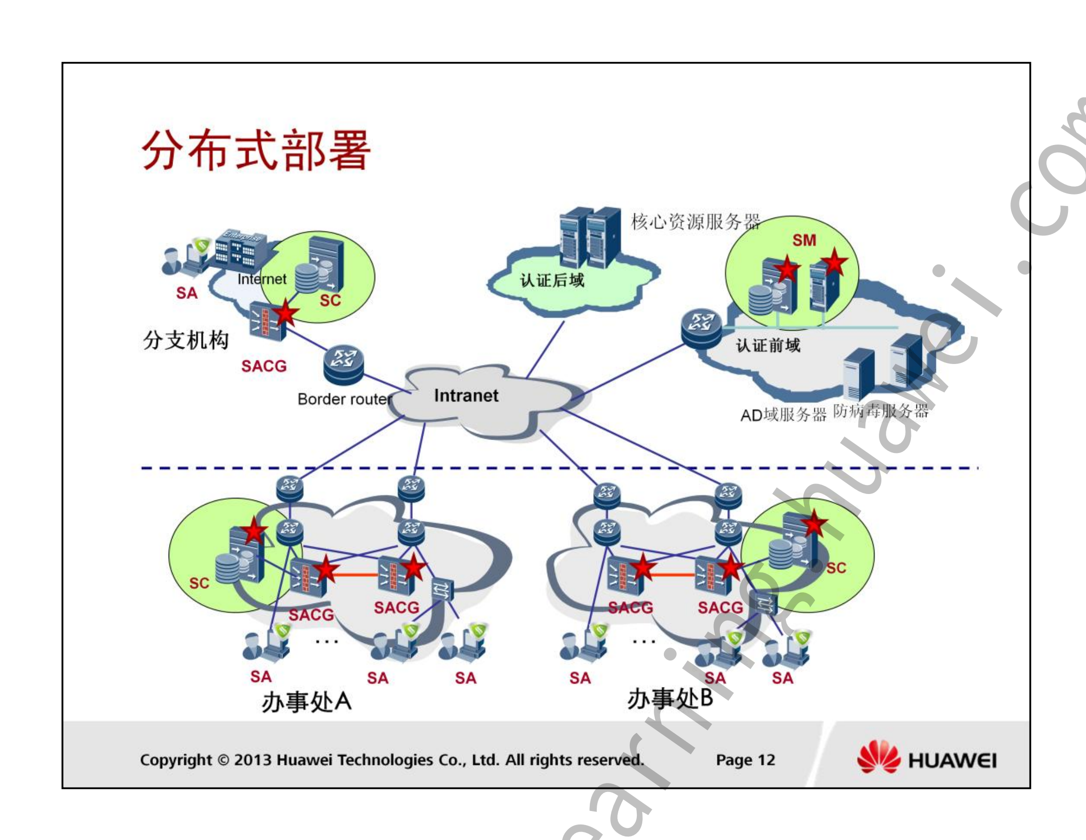
4、TSM系统区域与安全域关系：

1）认证前域和隔离域属于安全域中的服务域；

2）认证后域属于安全域中的业务域；



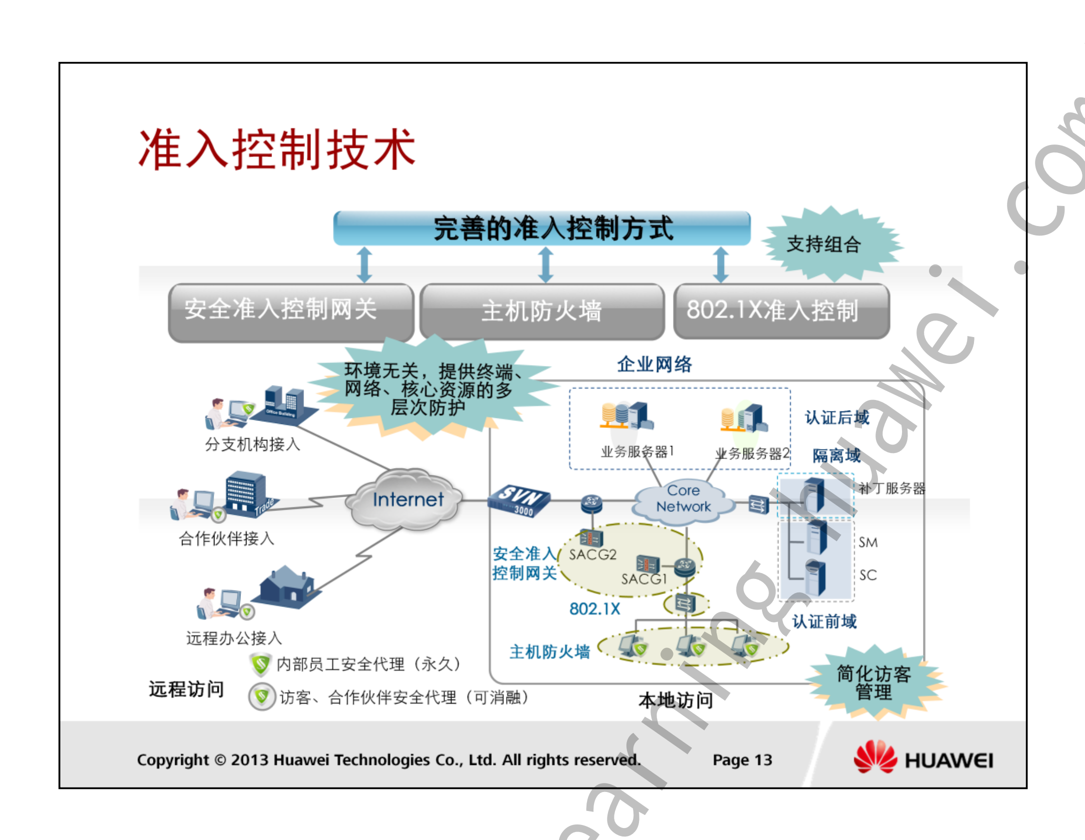
该部署方式的主要特点是将Secospace 服务器的集中部署，根据管理终端数目的多少，可以选择SM、SC、数据库等组件安装在同一台服务器上，也可选择分别安装，并可将SC做成群集方式以实现系统冗余（至少2台以上SC服务器）。SACG也可根据需要选择单机或者双机热备。



如果遇到下面的情况，建议采用分布式组网：

1. 终端相对集中在几个区域，而且区域之间的带宽比较小，由于代理与服务器之间存在一定的流量，如果采用集中式部署，将会占用区域之间的带宽，影响业务的提供；
2. 终端的规模相当大，可以考虑使用分布式组网，避免大量终端访问TSM服务器，占用大量的网络带宽；

分布式部署的时候， TSM安全代理选择就近的控制服务器，获得身份认证和准入控制等各项业务。



目前,业内提供NAC方案的厂商运用的准入控制方式主要包括：网关、802.1X、DHCP、主机防火墙、ARP等方式。

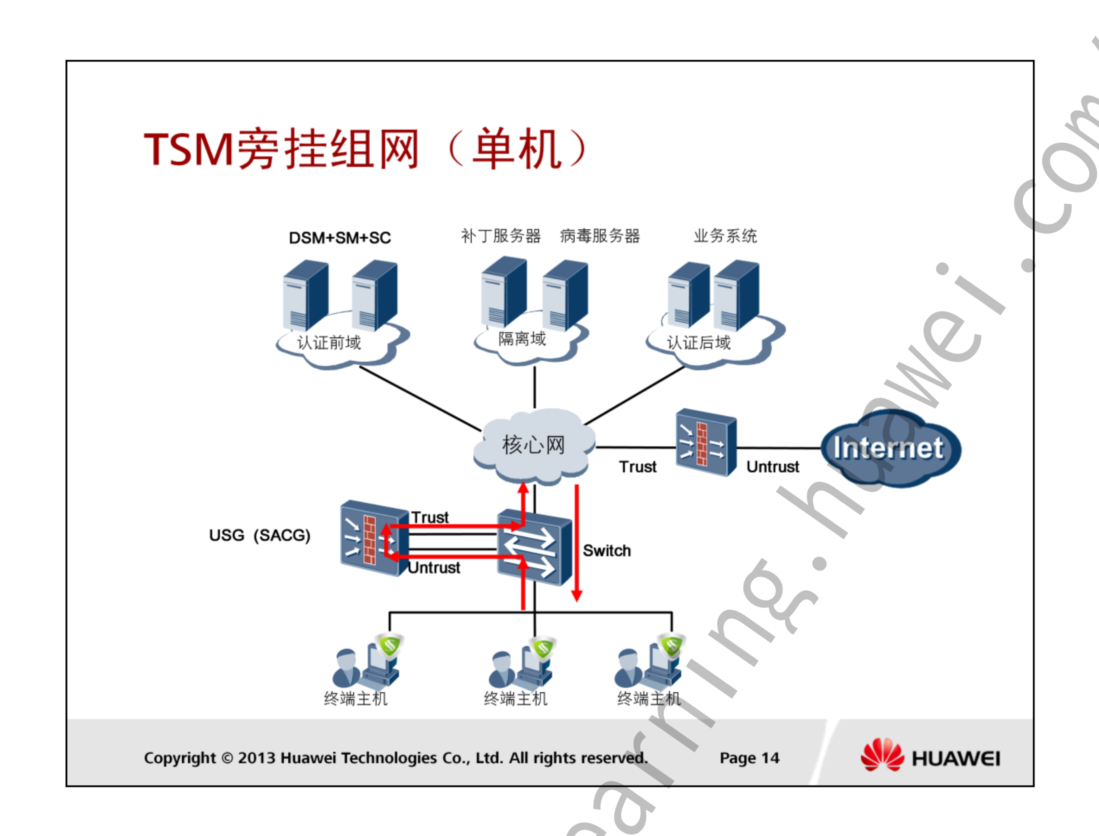
现在TSM支持多种准入控制方式，包括网关、802.1X和主机防火墙方式。

通过这三种强大的准入控制手段，基本能覆盖和适应所有典型案例的准入控制需求，包括内部雇员,分支机构,访客\远程办公等不同角色的不同准入控制，如VPN\无线等。

三种准入控制方式既可独立部署又可组合实施，如硬件SACG+主机防火墙、或硬件SACG+802.1X，能够有效实施严格的准入控制，同时成为解决同网段终端互访问题的最佳途径。

可消融代理：目前通过ActiveX插件实现，免安装和卸载。

前域只有一个，隔离域和后域支持多个，可以给不同部门或用户指定。



旁挂模式是指将SACG直接挂接在原有网络中的核心交换机或路由器上，实现TSM功能的组网模式。旁挂模式可以在不影响用户原有组网的前提下完成TSM功能的部署。

为建立访问权限管理机制，根据员工的工作需要授予不同的访问权限，保护企业核心网络资源，可以将USG作为TSM的SACG，与TSM联动部署。

- 主要实现如下需求：
  - 部署了两台TSM控制器，当USG与两台TSM控制器均无法联动时，USG将不对终端主机控制，终端主机全部放行。
  - 内网的终端主机上均已安装TSM代理软件，但是为了使某些临时来访人员也可以进行认证，所以也需要配置未安装TSM代理的终端用户通过Web方式认证。
  - 用户角色不同，能访问的网络资源也不同。以账号UserA为例，只允许l UserA访问“业务系统”，禁止访问其他认证后域资源。
  - 当终端用户身份认证通过，安全认证未通过时，需要在隔离域中修复，如下载补丁、更新病毒库。

TSM旁挂组网（双机）

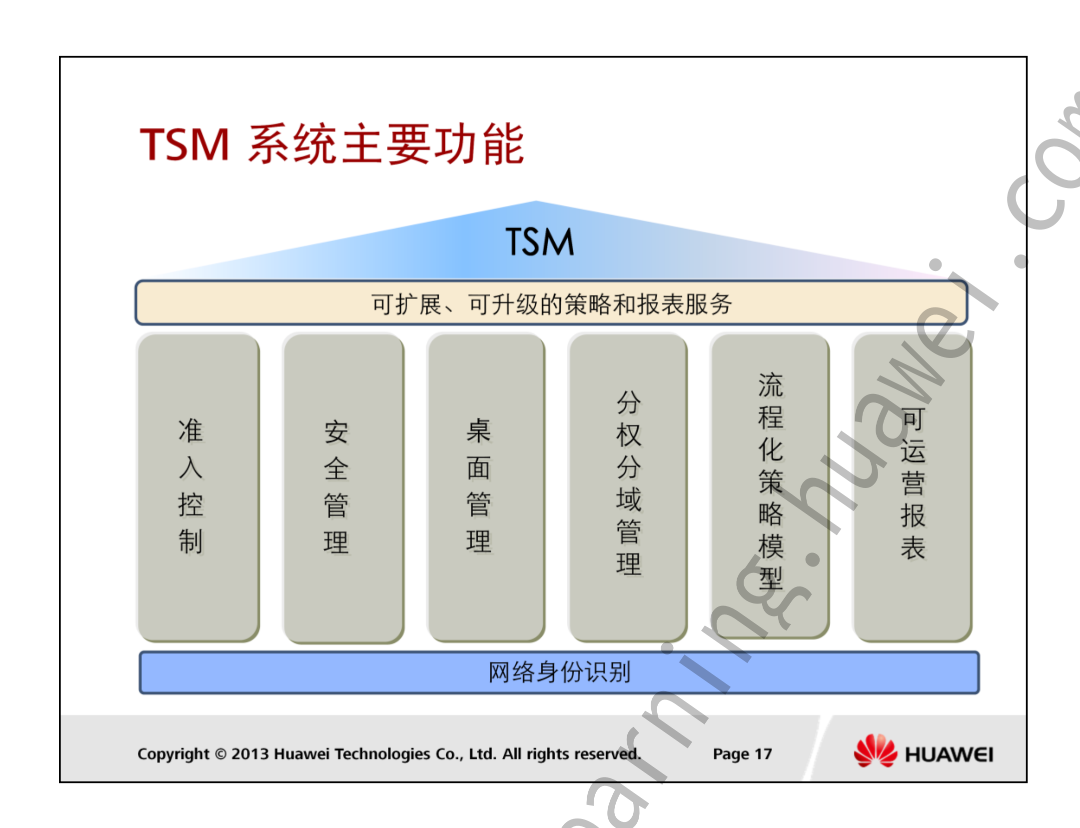
DSM+SM+SC
补丁服务器 病毒服务器
业务系统
认证前域
隔离域
认证后域
SACG1
(USG)
SACG2
(USG)
核心交换机1
核心交换机2
SACG心跳链路
回注链路（Trust）
引流链路（Untrust）
备份链路

Page 15
HUAWEI

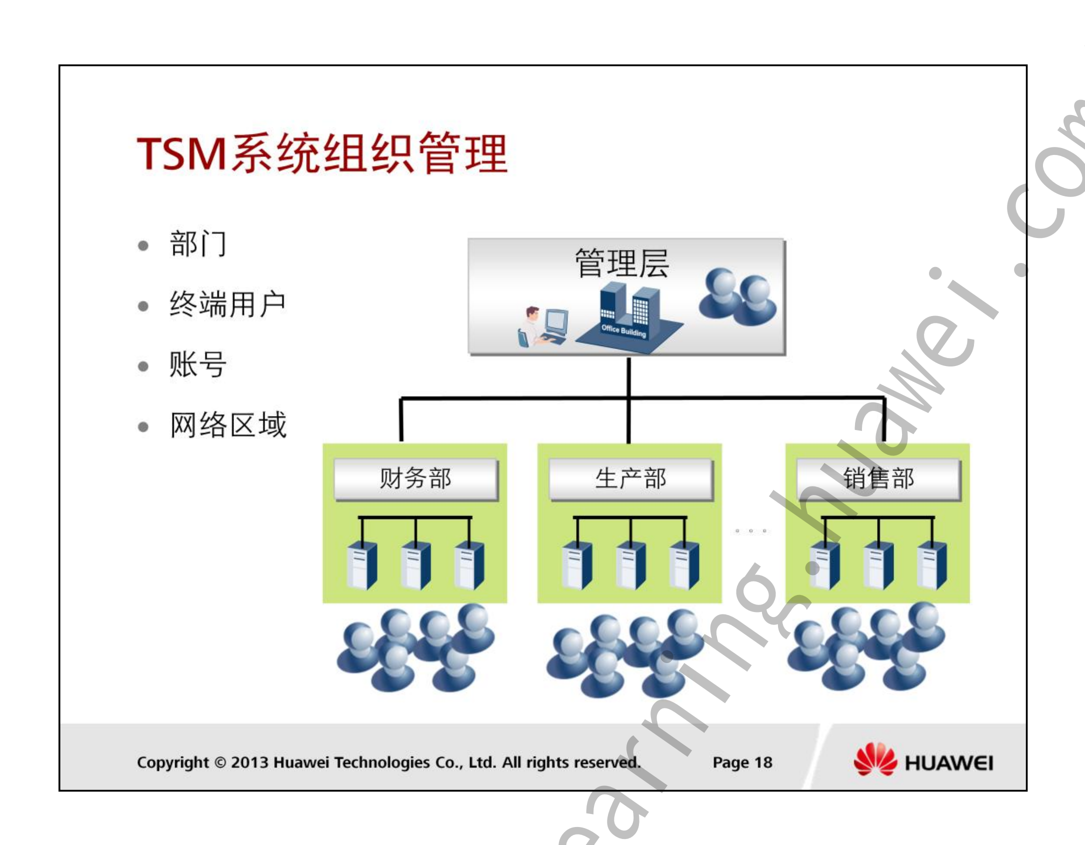


1. 终端安全概述
2. 终端安全系统部署
3. **终端安全策略部署**





- 准入控制包括：
    - 访客管理、例外设备管理、强制遵从性评估、授权用户访问范围
    - 身份认证、合规性检查、一键式自动修复、基于时段的NAC
- 安全管理包括：
    - 安全加固、办公行为管理
    - 自定义各种安全策略、信息泄密防护
    - 网络防护
- 桌面管理包括：
    - 补丁管理、资产管理
    - 软件分发、远程协助
    - 消息公告

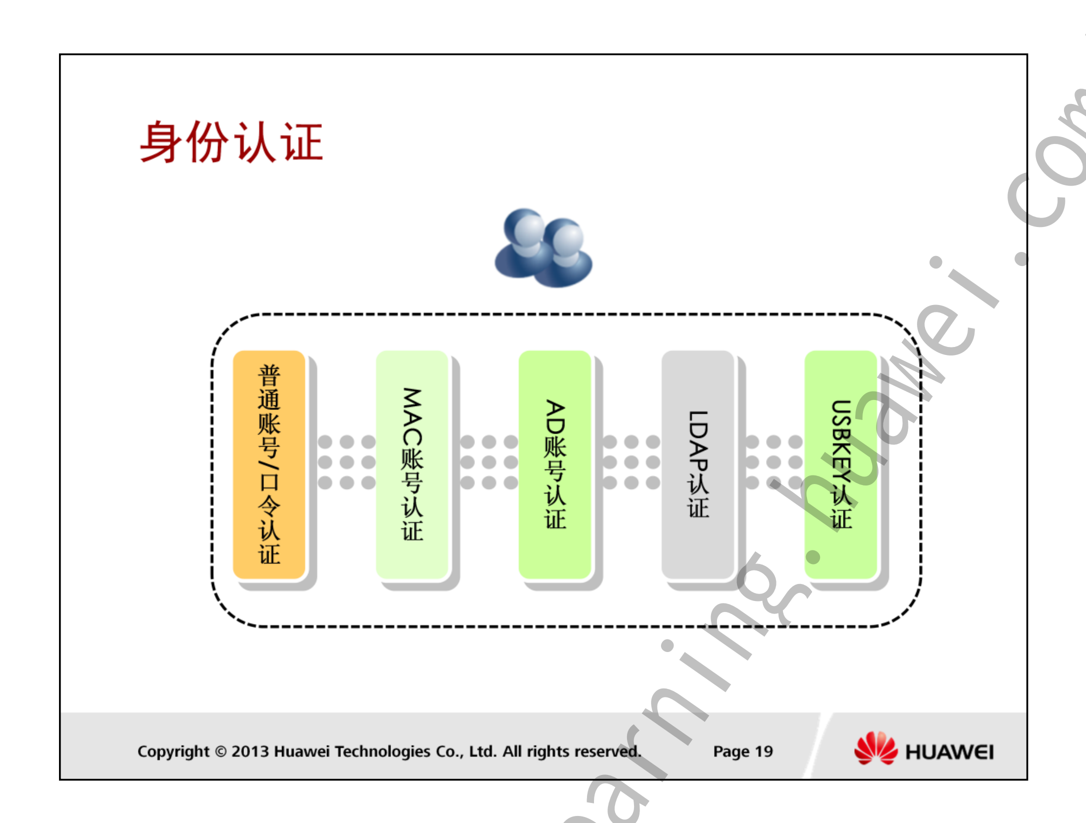


TSM系统支持层级管理的组织结构，系统中一个部门对应于企业中的一个部门，支持集中管理、分布管理和分级管理。

TSM系统实现对企业或部门内部的员工信息进行集中维护和管理。用户名可以重名，即使同一部门下，用户名也可以重名；在用户/账号批量导入的时候做了限制，同一部门下同名用户不能导入。

在访问企业内部的公共资源前，员工需要向管理员申请账号，员工在TSM代理、Web Agent插件或Web客户端输入账号进行身份认证，通过身份认证和安全认证后员工才能访问企业内部的公共资源。用户账号全局唯一，包括系统内建的账号，以及从外部数据源同步过来的账号。

TSM系统可以通过对企业内部的IP地址进行管理，实现各项业务与企业内部的IP地址绑定，从而实现企业内网安全的目的。基于网络区域管理是一种与基于部门管理不同的管理模式，它不区分用户的部门，而是根据用户所在的地域（IP地址），分区进行管理。



- 普通账号/口令认证
  - 终端用户在访问受控网络前，使用普通账号进行身份认证
- MAC账号认证
  - 终端主机在访问受控网络前，使用本机的MAC地址进行身份认证
- AD账号认证
  - 网络中已经部署了Microsoft AD域控制器，终端用户使用Microsoft AD域账号进行身份认证并接入受控网络
- LDAP认证
  - 网络中已经部署了LDAP认证服务器，终端用户使用现有的LDAP账号进行认证
- 支持USBKEY认证
  - 终端用户在访问受控网络前，使用移动证书进行身份认证

安全策略-共享目录检查

设置共享账号违规权限的信息：

增加 删除 导入 导出

		共享账号名称(用户或组)	账号违规的权限	违规等级	操作
1	☑	Everyone	写权限,完全控制	一般	

第 1 页 共 1 页

修复建议：

修复链接：

修改检查共享目录的账号

*共享账号名称(用户或组)：Everyone

账号违规的权限：☐ 读权限/读者 ☑ 写权限/参与者 ☑ 完全控制/共有者

*违规等级：一般

说明：
- 在Vista系统下读者即只读权限,参与者即写权限,共有者即完全控制权限。

确定 取消

 Page 20 HUAWEI

提供终端共享目录检查功能，检查终端PC设置共享目录的情况，支持检查以什么账号设置共享，以及该账号共享的权限。

检查内容如下：

- 共享账号名称（用户或者用户组）
- 违规共享权限：“读权限/读者”、“写权限/参与者”、“完全控制/共有者”
- 提供自动修复功能，删除违规共享

安全策略-检查打印机共享

检查打印机共享

保存 重置

策略名称： 检查打印机共享

策略描述： 检查本地打印机共享的账号以及权限是否符合要求，并提供自动修复功能。

策略执行参数

☑ 在终端显示策略检查结果　☐ 出现严重违规则禁止接入网络

☑ 启用自动修复　☐ 客户端启动时开始执行(系统默认为认证后开始执行)

检查周期为(分钟): 60

☑ 允许终端共享本地打印机

策略违规等级: 一般

共享账号违规权限信息表:

增加 删除 导入 导出

	共享账号名称（用户或组）	不允许拥有的权限	违规等级	操作
1	Everyone	打印,管理打印机,管...	一般	

第 1 页 共 1 页　1 - 1，共 1 条

修复建议:

修复链接:

 Page 21 HUAWEI

- 检查打印机共享目的
  - 检查安装在本地的打印机是否共享给其他人使用
  - 检查终端是否开启打印机共享，以及是否限制共享权限
- 检查的内容
  - 是否开启打印机共享
  - 检查打印权限共享给哪些账号
  - 检查打印机共享的权限：打印、管理打印机、管理文档
- 提供自动修复功能
  - 自动修复的时候，删除特定账号的共享，而不是关闭共享

安全策略-监控USB存储设备

监控USB存储设备

保存 重置

监控USB存储设备说明

策略名称： 监控USB存储设备

策略描述： 监控终端USB存储设备的访问，并提供文件监视功能。

策略执行参数

◯ 禁用移动存储设备 ◯ 移动存储设备只读 ◯ 监控移动存储设备 ◉ 移动存储设备写入加密

☑ 在终端显示策略检查结果

☑ 记录移动存储设备的插拔事件

☐ 允许离线解密

☑ 客户端启动时开始执行(系统默认为认证后开始执行)

☐ 移动存储设备禁用或只读时提示用户

 Page 22 HUAWEI

支持只禁用USB存储设备，即允许使用USB鼠标/键盘之类的非存储设备，而对于U盘/USB硬盘/USB光驱之类的存储设备完全禁用；

支持USB设备只读控制，即允许使用USB非存储设备，以及USB存储设备，对于USB存储设备，只允许读操作，禁止写操作；

提供USB设备文件操作的监控能力，能够识别并且记录文件操作；

在启用加密写功能后，终端用户拷贝到U盘的文件都是经过加密的，只有该企业的用户并且安装了TSM安全代理的终端，才能使用这些加密文件，加密文件从U盘拷贝到本地硬件自动解密。

安全策略-计算机外设监控

监控系统设备

保存 重置

监控系统设备说明

策略名称： 监控系统设备

策略描述： 提供对终端蓝牙设备、红外设备、SD控制器等系统设备的禁用功能。

策略执行参数

☑ 在终端显示策略检查结果 ☐ 客户端启动时开始执行(系统默认为认证后开始执行)

☑ 禁用设备时提示用户

禁用系统设备

☐ 串口 ☐ 并口 ☐ 红外设备

☐ 1394控制器 ☐ Modem ☐ SD/MMC控制器

☐ 软驱 ☐ 打印机 ☐ 蓝牙设备

☐ PCMCIA卡

策略违规等级: 一般

 Page 23 HUAWEI

支持软驱/串口/并口/红外/1394/Modem/PCMCIA/蓝牙/SD/MMC卡/本地打印机等计算机外设的监控功能，支持配置禁止外部设备。

当检查到外部设备或者接口的状态与策略配置不同，记录该事件，以及记录是否禁用成功；当检查到用户尝试启用被强制禁用的设备，记录该事件。

安全策略-检查端口

检查端口

保存 重置

☑ 在终端显示策略检查结果　　☐ 出现严重违规则禁止接入网络

☐ 客户端启动时开始执行(系统默认为认证后开始执行)

设置检查周期为(分钟): 60

禁止开放的端口列表:

增加 删除 导入 导出

	端口	协议	操作
1	80	TCP	

第 1 页 共 1 页　　1 - 1，共 1 条

☐ 只检查为LISTENING状态的端口

策略违规等级: 一般

修复建议:

修复链接:

HUAWEI

- 检查端口的目的：

  通过检查主机侦听的端口，判断主机是否安装了什么软件，例如通过该功能，可以检查主机是否开启DHCP服务。

- 功能说明：
  - 可以只检查侦听端口，也可以检查所有端口，包括处于TIME_WAIT类的端口；
  - 周期对终端的端口进行检查，检查的周期可以配置。

安全策略-监控DHCP设置

监控DHCP设置

保存 重置

监控DHCP说明

策略名称： 监控DHCP设置

策略描述： 监控终端DHCP属性的设置情况，并提供自动修复功能。

策略执行参数

☑ 在终端显示策略检查结果　☐ 出现严重违规则禁止接入网络

☐ 启用自动修复　☐ 客户端启动时开始执行(系统默认为认证后开始执行)

☐ 强制使用DHCP协议　☐ 强制使用DHCP协议时提示用户

◉ 检查所有网卡　○ 仅检查连接TSM服务器网卡　○ 检查与TSM服务器连接之外的网卡

策略违规等级: 一般

修复建议:

修复链接:

 Page 25 HUAWEI

- 监控DHCP设置说明
  - 检查终端是否使用DHCP获得IP地址。
  - 允许强制终端必须使用DHCP获得IP地址，并且不允许终端用户手工修改（把TCP/IP协议的”属性“按钮禁用）。
  - 检查所有的网卡
  - 仅检查连接SC控制服务器的网卡（离线的情况下，由于无法判断哪个网卡连接服务器，在此选项情况下，不检查）；
  - 仅检查不连接SC控制服务器的网卡（离线的情况下，由于无法判断哪个网卡连接服务器，在此选项情况下，不检查）。

安全策略-非法外联

发现非法外联后的控制方式: 提示用户，并记录非法外联事件

○ 允许通过合法路径连接外网 ◉ 禁止访问互联网

目标地址或域名,如：172.168.100.188:80(用";"分隔多个地址):

Web重定向服务器IP地址,如：172.168.100.188(用";"分隔多个地址):

说明：
- 在配置允许通过合法路径连接外网时,如果终端到外网目的IP没有经过合法的路由IP,则认为该终端存在非法外联。
- 在配置禁止访问互联网时,如果终端到可以与目标地址建立连接,则认为该该终端存在非法外联;如果局域网中存在web重定向时，如防火墙web推送，需要配置web重定向服务器地址，避免非法外联检查错误。

 Page 26 HUAWEI

提供无合法外联途径的外联监控功能，支持主动探测指定外网地址，防止任何形式的外网连接;

提供有合法外联途径的外联监控，支持探测指定外网地址，若没有经过指定的合法的网络出口，则上报服务器。

安全策略-检查防病毒软件

修改检查的杀毒软件

*软件厂商: Kingsoft
*软件名称: Kingsoft Internet version 5.0-5.5
*软件版本: 2008-5-23
*病毒库更新周期(天): 15
是否自动修复: 是 否
请求自动修复后容许接入网络
是否认证后杀毒: 是 否
认证后开始杀毒(分钟):
发现不能查杀的病毒作为严重违规
杀毒路径: 内存
系统目录(如: C:\Windows\System)
自定义路径(多个路径以竖线 | 分隔)

 Page 27 HUAWEI

对江民、金山的企业杀毒软件供防病毒软件的强联动功能，提供自动修复功能，自动更新病毒库；支持认证后启动杀毒功能，能够定义启动后扫描病毒的路径，包括内存/系统目录，以及自定义的路径等，当终端存在无法查杀的病毒时，与接入控制设备联动对终端进行隔离。

支持强联动杀毒软件：

- 金山毒霸2006、2007、2009
- 江民KV2008，KV2009, KV2010, KVNET2008, KVNET2009, KVNET2010
- Symantec AntiVirus 10.0企业版、Endpoint Protection 11.0
- Rising AntiVirus Software 2006、2007、2008、2009、Internet Security 2009
- 卡巴斯基反病毒软件 6.0、7.0、2009、反病毒软件工作站 5.0
- ……

除以上所支持的强联动杀毒软件外，还支持弱联动杀毒软件为业界主流杀毒软件，相关信息请见最新版本产品文档。

安全策略-补丁检查

配置补丁检查内容

操作系统补丁等级	违规等级	
☑ 关键	○ 严重	◉ 一般
☑ 重要	○ 严重	◉ 一般
☐ 中	○ 严重	◉ 一般
☐ 低	○ 严重	◉ 一般
☐ 未知	○ 严重	◉ 一般

说明：
- 以上补丁违规等级配置需要联动
- 需要联动的配置项，只有启用WSUS联动或TSM补丁管理才生效，下同。

补丁列表:

增加补丁 删除补丁 导入 导出

☐	知识库号	补丁适用操作系统	违规等级	修复建议	下载链接	操作

第 1 页 共 1 页

无需检查的例外补丁(需要联动)

增加例外补丁 删除例外补丁 导入 导出

☐	知识库号	补丁适用操作系统	操作

第 1 页 共 1 页

Page 28

HUAWEI

1. 根据补丁的级别检查终端PC是否安装了特定级别的补丁，补丁级别包括关键、严重、重要、一般、未知；（全功能模块）
2. 根据补丁列表检查终端PC是否安装了某个补丁；
3. 提供例外补丁列表，允许某些补丁不检查，当存在冲突的时候，以例外补丁列表的要求为准；
4. 支持配置修复建议和修复连接，实施手工修复；
5. 支持自动修复。



总结

- 什么是终端安全
- TSM系统的组成部分及如何部署
- TSM系统组织管理和准入控制方式
- TSM系统的安全策略配置



思考题

- TSM是什么？它能解决哪些终端安全问题？
- TSM系统主要由哪些组件组成？
- SM、SC组件在TSM系统中各承担什么角色，那个组件与SACG有业务交互？
- TSM系统有哪2种管理维度？它们之间有何区别？
- TSM系统可支持哪些身份认证方式？它们之间有何区别？
- TSM系统主要有哪些安全策略？这些安全策略各解决什么问题？



Thank you

www.huawei.com

华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*）享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的“华为账号”和注册账号的“email地址”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训->面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- **4、学习工具 eNSP**
  - *eNSP (Enterprise Network Simulation Platform)*，是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。**您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。**（http://support.huawei.com/ecommunity/bbs/list_2247.html）

